AUFTRAGSDATEN-VERARBEITUNG

DAS FORDERT DIE DSGVO

PRIVACYXPERTS

Inhaltsverzeichnis

Auftragsdatenverarbeitung: Das fordert die DS-GVO 3

Auftragsverarbeiter - Das müssen Sie wissen 4

CHECKLISTE: AUFTRAGSVERARBEITUNG 5

Sonderfall: Wartung und Fernzugriffe 9

Sonderfall: Auftragsverarbeitung außerhalb der EU-/EWR 10

Auftragsverarbeiter: Das sind die Vorschriften 11

Haftung: Dafür haften Auftragsverarbeiter wirklich 12

Verträge mit Auftragsverarbeitern: Diese Anforderungen müssen Sie kennen 13

CHECKLISTE: VERTRAGSANFORDERUNGEN FÜR AUFTRAGSVERARBEITUNGEN NACH ART. 24 DS-GVO (!) 14

Subunternehmer: Das müssen Sie beachten 15

Exkurs: Datenschutzkultur 16

Zum Wohle der Betroffenen 16

Verpflichtung auf den Datenschutz 17

Datenschutzleitlinie 17

TOM: Diese Maßnahmen müssen Sie fordern 21

Mythos und Wahrheit: Kennen Sie sich mit der Auftragsverarbeitung aus? 23

PRIVACYXPERTS

Auftragsdatenverarbeitung: Das fordert die DS-GVO

Nach einer aktuellen Studie des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) sehen Unternehmen den schwer abzuschätzenden Aufwand (42 %) und die Rechtsunsicherheit (52 %) als größte Herausforderung bei der Umsetzung der DS-GVO an.

Daraus resultiert auch die Tatsache, dass noch immer jedes dritte Unternehmen in Deutschland die DS-GVO ignoriert. Da die meisten Unternehmen mit IT-Dienstleistern oder anderen Auftragsverarbeitern zusammenarbeiten, gehen die Unternehmen gerade in diesem sensiblen Bereich hohe Risiken ein. Denn Datenschutz und Datensicherheit kosten Geld, das der Dienstleister oftmals nicht investieren. Vielfach weil die Kunden dafür nicht zahlen wollen. Hier schließt sich ein Teufelskreis, auf den Sie als Datenschutzbeauftragter Ihre Geschäftsleitung und Ihre Auftragsverarbeiter hinweisen müssen. Denn nur wenn beide Parteien gemeinsam daran arbeiten, die Anforderungen der DS-GVO umzusetzen, und auch bereit sind, dafür zu investieren, können existenzbedrohende Bußgelder und Schadensersatzforderungen verhindert werden.

Jetzt können Sie sich jede Menge Arbeit sparen …

Weil dieses Thema so kompliziert und arbeitsintensiv ist, haben wir **speziell für Sie als Datenschutzbeauftragten** einen **Zeitspar-Ratgeber zum Thema „Betroffenenrechte: Auskunft und Löschung“** erstellt, der Ihnen Antworten auf die häufigsten Fragestellungen liefert.

Aber nicht nur das: Sie finden darin auch Formulierungsmuster, etwa für eine **Zwischeninformation** des Betroffenen oder die **Anforderung eines Identitätsnachweises**.

Sichern Sie sich jetzt das für Sie reservierte Exemplar mit zahlreichen Tipps, Praxishinweisen, Mustern, Erklärungen und Antworten.

Hier können Sie den Ratgeber „Betroffenenrechte: Auskunft und Löschung“ jetzt gleich kostenlos anfordern.

Das sind die Themen des Ratgebers „Betroffenenrechte: Auskunft und Löschung“:

- Stichwort Betroffenenrechte: **Antworten auf die wichtigsten Fragen**
- **Zwischeninfo und Identitätsnachweis:** So können Ihre Standardschreiben an die Betroffenen aussehen
- **Umfang des Auskunftsanspruchs:** Diese Fakten und Urteile müssen Sie kennen
- **Recht auf Löschung:** So setzen Sie es im Unternehmen wirksam um
- Mit diesem **Musteranschreiben informieren Sie alle Mitarbeiter über die Rechte der Betroffenen**

Klicken Sie jetzt hier, um sich den Ratgeber „Betroffenenrechte: Auskunft und Löschung“ jetzt gleich kostenlos zu sichern.. »

Holen Sie sich jetzt wichtiges Praxis-Knowhow zu Betroffenenrechten

BEST SELLER

Mit dem kostenlosen Spezialreport erhalten Sie praktische Schritt-für-Schritt-Anleitungen, Muster und viele wertvolle Tipps, um das Thema sofort in die Praxis umzusetzen.

Testen Sie „Datenschutz aktuell“ noch heute völlig kostenlos! Der Spezialreport steht Ihnen sofort kostenlos als PDF-Datei zur Verfügung »

Zusätzlich zu diesem Spezialreport erhalten Sie:

Eine Ausgabe von "Datenschutz aktuell" kostenlos zum Testen

MEIN TIPP:

Als Datenschutzbeauftragter sollten Sie Ihre Geschäftsleitung auch dahingehend sensibilisieren, dass das Unternehmen eine hohe Verantwortung für die Rechte der Betroffenen hat. Schließlich geht es nicht nur um Geld, sondern auch um die Grundrechte der Beschäftigten und Kunden.

Auftragsverarbeiter - Das müssen Sie wissen

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Wobei der Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO die Stelle ist, die allein oder gemeinsam mit anderen Stellen über Art und Umfang der Datenverarbeitung entscheidet. Die Verantwortung bezieht sich maßgeblich auf die Festlegung der Verarbeitungszwecke. Entscheidungen zu konkreten Fragen über die technischen und organisatorischen Maßnahmen (TOM) können hingegen an den Auftragsverarbeiter delegiert werden.

Der Auftragsverarbeiter muss die TOM auch in der betrieblichen Praxis umsetzen. Das bedeutet jedoch nicht, dass der Verantwortliche dem Auftragsverarbeiter nicht in einem Vertrag zur Auftragsdatenverarbeitung (ADV) klare Vorgaben in Hinsicht auf die zu erfüllenden grundsätzlichen Sicherheitsanforderungen geben sollte. Dem Auftragsverarbeiter verbleibt aber dennoch ein gewisser Entscheidungsspielraum, wie er diese Anforderungen in seiner betrieblichen Praxis konkret umsetzt.

Auftragsverarbeiter müssen nach Art. 30 Abs. 2 DS-GVO auch ein eigenes Verzeichnis von Verarbeitungstätigkeiten für alle Kategorien der im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten führen. Dieses Verzeichnis muss der Auftragsverarbeiter gemäß Art. 33 Abs. 2 DS-GVO der Aufsichtsbehörde auf Anfrage zur Verfügung stellen. Dieses Verarbeitungsverzeichnis ist eine gute Basis für Ihre Kontrollen beim Auftragsverarbeiter.

Als Datenschutzbeauftragter müssen Sie immer dann, wenn personenbezogene Daten bei der Übertragung einer Aufgabe auf eine dritte juristische Person betroffen sind, prüfen, ob es sich dabei um eine Auftragsdatenverarbeitung handelt. Dabei spielt es keine Rolle, ob die Aufgabe innerhalb oder außerhalb des Unternehmens oder einer Unternehmensgruppe übertragen wird. Mit der nachfolgenden Checkliste können Sie eine solche Prüfung durchführen.

CHECKLISTE: AUFTRAGSVERARBEITUNG

Übertragung von Aufgaben	Ja	Nein
Bezieht sich die Dienstleistung im Wesentlichen auf die Verarbeitung personenbezogener Daten für Zwecke des Auftraggebers und besteht kein eigenes Interesse des Dienstleisters an den Daten?	☐	☐
Legt Ihr Unternehmen die Zwecke und Mittel der Verarbeitung im Wesentlichen fest?	☐	☐
Hat der Auftragsverarbeiter ausschließlich eine technische Hilfs- oder Unterstützungsfunktion?	☐	☐
Fehlt dem Auftragsverarbeiter die Entscheidungsbefugnis über die Daten?	☐	☐
Verfolgt der Auftragsverarbeiter mit der Datenverarbeitung keine eigenen Zwecke?	☐	☐
Unterliegt der Auftragsverarbeiter einem ausdrücklichen Nutzungsverbot in Bezug auf die zu verarbeitenden Daten?	☐	☐
Wird die Datenverarbeitung nach außen hin vom Auftraggeber verantwortet?	☐	☐
Steht der Auftragsverarbeiter in keinerlei vertraglichen Beziehungen zu den von der Datenverarbeitung Betroffenen?	☐	☐

Haben Sie eine der Fragen bejaht, können Sie in der Regel von einer Auftragsverarbeitung ausgehen.

Beispiele für typische Auftragsverarbeitungen sind:

- Rechenzentrumsbetrieb für Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung
- Cloud-Computing mit personenbezogenen Daten, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist
- Werbeadressenverarbeitung in einem Lettershop
- Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume des Dienstleisters
- Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Internetportalen (z. B. Betreuung von Kontaktformularen oder Nutzeranfragen)
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten (elektronische Personalakte, Vertragsverwaltung, elektronische Post usw.)
- Auslagerung von Backup-Daten und anderer Archivierungen
- Datenträger- oder Papierentsorgung durch Dienstleister Prüfung oder Wartung (z. B. Fernwartung, externer Support) von IT-Systemen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
- Inanspruchnahme von Druckdienstleistungen
- Zentralisierung bestimmter Prozesse innerhalb eines Konzerns, wie Personalwesen, Reisekostenabrechnung usw., sofern kein Fall gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO vor liegt

Beispiele für die Inanspruchnahme fremder Fachleistungen mit einem eigenständigen Verantwortlichen sind:

- Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer, Gutachter usw.
- Inkassobüros mit Forderungsübertragung
- Banken für Zahlungsverkehr
- Postdienste für Brieftransport

MEIN TIPP:

Prüfen Sie als Datenschutzbeauftragter immer, ob der Auftragsverarbeiter im Wesentlichen unterstützende Funktionen übernimmt und den Weisungen Ihres Unternehmens unterworfen ist. Handelt der Auftragsverarbeiter hingegen auch bei der Festlegung von Zwecken und Mitteln selbstständig und werden ihm z. B. vollständige Geschäftsprozesse über tragen, wird der Auftragsverarbeiter selbst zum Verantwortlichen. Die Grundlage für eine solche Datenübermittlung findet sich in Art. 6 Abs. 1 lit. f DS-GVO und umfasst die Wahrung der berechtigten Interessen.

Der Auftragsverarbeiter ist nach Art. 29 DS-GVO weisungsgebunden und ist daher kein Dritter im Sinne des Art. 4 Nr. 10 DS-GVO. Die Datenverarbeitung durch den Auftragsverarbeiter findet demnach in einem Innenverhältnis statt und ist dem Verantwortlichen zugerechnet. In diesem Innenverhältnis bedarf es bei einer Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter keiner weiteren Rechtsgrundlage als der, auf die sich der Verantwortliche selbst bezieht. Auftragsverarbeiter sind jedoch im Sinne von Art. 9 DS-GVO Empfänger von Daten. Dies führt gemäß Art. 19 DS-GVO zu gesonderten Informations- und Mitteilungspflichten des Verantwortlichen. Ferner bestehen nach Art. 15 DS-GVO Auskunftsrechte der Betroffenen gegenüber dem Verantwortlichen.

MEIN TIPP:

Damit Ihr Unternehmen die vorgenannten Informations- und Mitteilungspflichten sowie die Auskunftsrechte der Betroffenen erfüllen kann, müssen Sie die Auftragsverarbeiter als Empfänger von Daten in Ihrem Verzeichnis der Verarbeitungstätigkeiten aufführen.

Sonderfall: Wartung und Fernzugriffe

Führt ein Dienstleister Wartungsarbeiten an IT-Systemen durch, kann in der Regel nicht ausgeschlossen werden, dass er Zugriff auf die darin gespeicherten personenbezogenen Daten hat. Gleiches gilt für Fernzugriffe auf IT-Systeme zu Wartungszwecken. In sofern spielt es keine Rolle, ob der Zugriff in den Räumlichkeiten des Verantwortlichen oder über Netzwerkverbindungen erfolgt.

Inwieweit es sich bei solchen Zugriffen auf personenbezogene Daten um eine Auftragsverarbeitung nach Art. 28 DS-GVO handelt, ist unter Datenschützern noch umstritten. Auch das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat sich in dieser Frage noch nicht festgelegt. Als Datenschutzbeauftragter sollten Sie risikoorientiert vorgehen und prüfen, in welchem Umfang der jeweilige Dienstleister auf personenbezogene Daten zugreifen kann. Greift ein IT-Dienstleister z. B. mit Administrationsrechten auf IT-Systeme mit personenbezogenen Daten zu, können Sie durchaus auf die weite Definition einer Verarbeitung in Art. 4 Nr. 2 DS-GVO abstellen (Auslesen, Abfragen, Verwenden). Ist Auftragsgegenstand der (Fern-)Wartung allerdings gerade der Umgang mit Datensätzen mit personenbezogenen Daten, handelt es sich in jedem Fall um eine Auftragsverarbeitung nach Art. 28 DS-GVO (BayLDA).

Dies ist z. B. bei der Durchführung und der Speicherung von Datensicherungen in den Räumlichkeiten des IT-Dienstleisters der Fall. Anders ist es bei der Wartung von rein technischen Systemen wie z. B. Klimaanlagen. Solche Dienstleistungen fallen nach wie vor nicht unter die Auftragsverarbeitung.

MEIN TIPP:

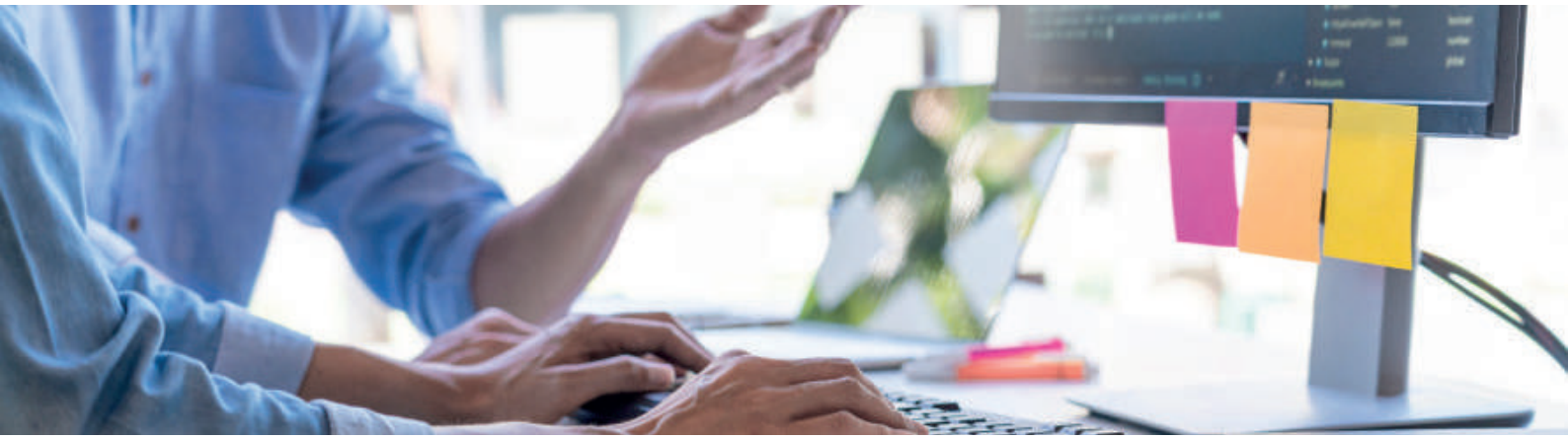
Als Datenschutzbeauftragter sollten Sie unabhängig davon, ob es sich bei einer Dienstleistung um eine Auftragsverarbeitung nach Art. 24 DS-GVO handelt oder nicht, darauf hinwirken, dass es verbindliche vertragliche Regelungen zur Umsetzung der von Ihnen geforderten TOM mit dem Dienstleister gibt. Hierzu zählt auch eine Verpflichtung auf das Datengeheimnis. Denn auch ein IT-Dienstleister, der Ihre IT-Systeme außerhalb einer Auftragsverarbeitung wartet, muss grundlegende Sicherheitsanforderungen umsetzen. Schließlich ist Ihr Unternehmen für die Einhaltung der datenschutzrechtlichen Anforderungen verantwortlich.

Sonderfall: Auftragsverarbeitung außerhalb der EU-/EWR

Nach der DS-GVO kann die Auftragsdatenverarbeitung auch außerhalb des EU-/EWR-Raums stattfinden. Hierbei sind allerdings zusätzliche Anforderungen der Art. 44 ff. DS-GVO für Datenverarbeitungen in Drittstaaten einzuhalten. Hierzu zählen im Wesentlichen die Einhaltung und der Nachweis eines angemessenen Schutzniveaus im jeweiligen Drittstaat gemäß Art. 45 DS-GVO oder geeignete Garantien nach Art. 46 DS-GVO wie z. B. Standardvertragsklauseln oder Ausnahmetatbestände nach Art. 49 DS-GVO.

Als Datenschutzbeauftragter müssen Sie bei Auftragsverarbeitern in Drittländern sehr genau prüfen, ob diese Voraussetzungen tatsächlich erfüllt sind und vertraglich abgesichert werden. In der Regel können Sie jedoch die Vertragsgestaltung mit großen Dienstleistern in Drittstaaten kaum beeinflussen. Insbesondere bei der Nutzung von Clouddiensten von Konzernen wie Amazon, Microsoft oder Apple werden Sie keine individuellen Verträge zur Auftragsdatenverarbeitung abschließen können. In solchen Fällen müssen Sie auf die Verarbeitung personenbezogener Daten in der Regel verzichten. Es gibt hier jedoch auch Sonderfälle, wie die eigens in Deutschland eingerichteten Rechenzentren von MS zusammen mit der Telekom, um den EU-Datenschutz-

anforderungen gerecht zu werden. Eine Möglichkeit, Verstöße gegen die DS-GVO zu vermeiden, stellt die Verschlüsselung der personenbezogenen Daten in der Cloud dar. Eine andere Möglichkeit ist die Nutzung von Dienstleistern, die ihre Cloud im europäischen Raum anbieten.



Auftragsverarbeiter: Das sind die Vorschriften

Verantwortliche müssen gemäß Art. 28 DS-GVO vor der Auftragsvergabe prüfen, ob der Auftragsverarbeiter geeignet ist. Wobei sich die Eignung darauf bezieht, ob der Auftragsverarbeiter hinreichende Garantien dafür bietet, dass er geeignete technische und organisatorische Maßnahmen (TOM) etabliert hat. Denn nur so kann die Auftragsdatenverarbeitung die Anforderungen der DS-GVO erfüllen.

Zum Beleg solcher Garantien können genehmigte Verhaltensregeln nach Art. 40 DS-GVO oder Zertifizierungen gemäß Art. 42 DS-GVO dienen. Als Datenschutzbeauftragter stehen Ihnen für Ihre Prüfungen aber derzeit noch wenige solcher genehmigter Verhaltensregeln von Branchenverbänden oder Zertifizierungen unabhängiger Stellen zur Verfügung. Sie müssen Ihre Auftragsverarbeiter also auf der Basis gängiger Sicherheitsstandards aus der Informationssicherheit prüfen.

Beispiele hierfür sind z. B. die ISO 27001 und die Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI), wie z. B. der Standard 100-1 oder die BSI Grundschutzkataloge.

Haftung: Dafür haften Auftragsverarbeiter wirklich

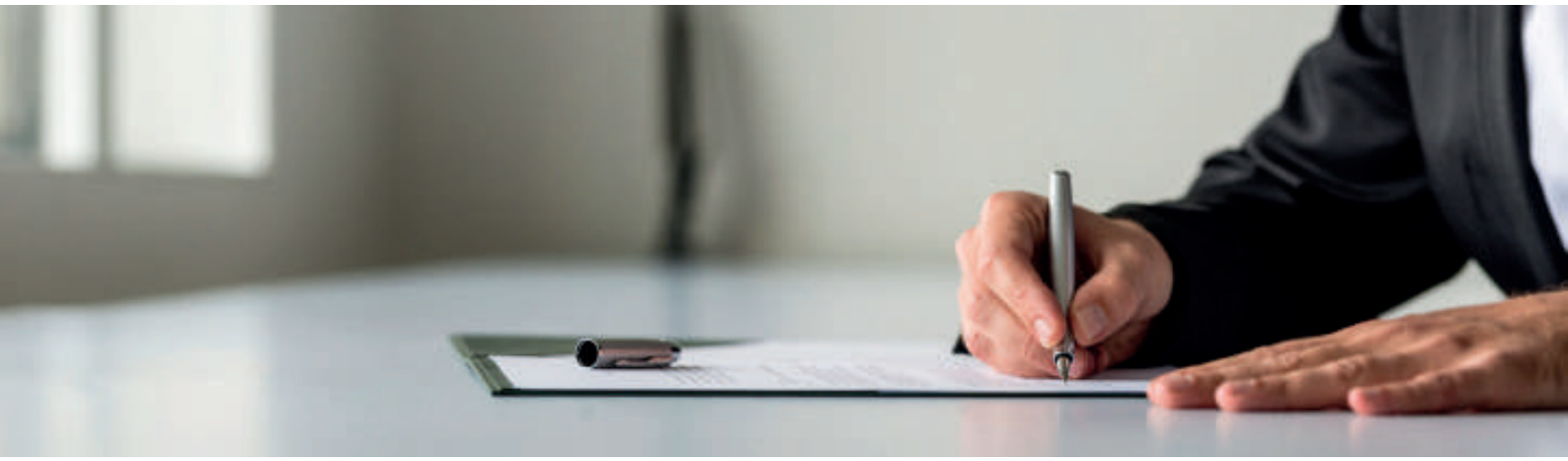
Angesichts existenzbedrohender Bußgelder oder zusätzlicher Schadensersatzforderungen seitens der Betroffenen bei Verstößen gegen die DS-GVO ist es wichtig, grundlegende Haftungsfragen bei der Auftragsverarbeitung zu kennen. Nach Art. 82 Abs. 1 DS-GVO haften Verantwortliche und Auftragsverarbeiter sowie alle eventuell an der Verarbeitung Beteiligten bei Schadensersatzansprüchen der Betroffenen gesamtschuldnerisch.

Nach dieser Rechtslage wird sich der Verantwortliche im Rahmen des Gesamtschuldnerinnenausgleichs am Auftragsverarbeiter unter Beachtung einer Verschuldensquote schadlos halten können, wobei der Auftragsverarbeiter nur für die Verstöße haftet, für die er im Rahmen der Auftragserfüllung tatsächlich verantwortlich ist. Die Haftung umschließt auch Verstöße gegen rechtmäßige Weisungen des Verantwortlichen. Sie sollten aber beachten, dass der Auftragsverarbeiter nicht für Pflichten haftet, die ihm vertraglich über die Anforderungen nach Art. 28 Abs. 3, 4 und 5 DS-GVO auferlegt sind.

Demnach verantwortet der Auftragsverarbeiter nur

- die weisungs- und zweckgemäße sowie mittelkonforme Verarbeitung der Daten, inkl. Hinweispflicht bei rechtswidrigen Weisungen,
- die Vertraulichkeitsverpflichtung der beteiligten befugten Personen,
- die ergriffenen technischen und organisatorischen Schutzmaßnahmen,
- die ordnungsgemäße Beauftragung von Unterauftragnehmern,
- die Mithilfe bei Wahrnehmung von Betroffenenrechten - soweit vereinbart,
- Unterstützung bei Meldung von Datenschutzvorfällen,
- Unterstützung bei Durchführung von Datenschutz-Folgenabschätzungen - soweit vereinbart,

- Erstellung und Führung eines Verarbeitungsverzeichnisses der Verarbeitungstätigkeiten im Rahmen der Auftragsverarbeitungen,
- die Bestellung eines eigenen Datenschutzbeauftragten,
- ordnungs- und vertragsgemäße Löschung und/ oder Rückgabe von Daten nach Abschluss der Verarbeitung,
- Duldung und Mitwirkung bei Prüfungen und Audits des für die Verarbeitung Verantwortlichen.



Verträge mit Auftragsverarbeitern: Diese Anforderungen müssen Sie kennen

Auftragsverarbeitungen mussten bereits nach § 11 BDSG (alt) vertraglich geregelt werden. Insbesondere die weisungsgebundenen Tätigkeiten mussten konkret geregelt werden. Für die Inhalte der Verträge gelten in großen Teilen die gleichen Regeln wie bisher. Bestehende Verträge können demnach fortgelten, wenn Sie der DS-GVO entsprechen. Hierbei müssen Sie prüfen, inwieweit der Altvertrag die TOM in ausreichendem Maße gemäß Art. 32 DS-GVO regelt und ob insbesondere der Einsatz von Subunternehmen geregelt ist. Mit der nachfolgenden Checkliste können Sie prüfen, ob Ihre Altverträge oder Neuverträge den Anforderungen der DS-GVO genügen.

CHECKLISTE: VERTRAGSANFORDERUNGEN FÜR AUFTRAGSVERARBEITUNGEN NACH ART. 24 DS-GVO (!)

	Geregelt?	
Vertragsinhalt	Ja	Nein
Gegenstand und Dauer der Verarbeitung	☐	☐
Art und Zweck der Verarbeitung	☐	☐
Art der personenbezogenen Daten	☐	☐
Kategorien betroffener Personen	☐	☐
Pflichten und Rechte des Verantwortlichen	☐	☐
Umfang der Weisungsbefugnisse des Auftraggebers (Verantwortlicher)	☐	☐
Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit	☐	☐
Mitteilungspflichten des Auftragnehmers (Auftragsverarbeiter) bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten	☐	☐
Sicherstellung von technischen & organisatorischen Maßnahmen nach Art 32 DS-GVO	☐	☐
Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)	☐	☐
Unterstützung des Verantwortlichen bei Anfragen und Ansprüchen Betroffener	☐	☐
Unterstützung des Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung	☐	☐

Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung	☐	☐
Regelung wie der Nachweis der Einhaltung der in Art. 28 und Art. 32 niedergelegten Pflichten erfolgt. Dies kann auch durch Überprüfungen und Inspektionen durch einen beauftragten Prüfer vereinbart werden (Prüfungsrechte)	☐	☐
Pflicht des Auftragsverarbeiters, den Verantwortlichen unverzüglich zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt	☐	☐
Haftungsfragen	☐	☐

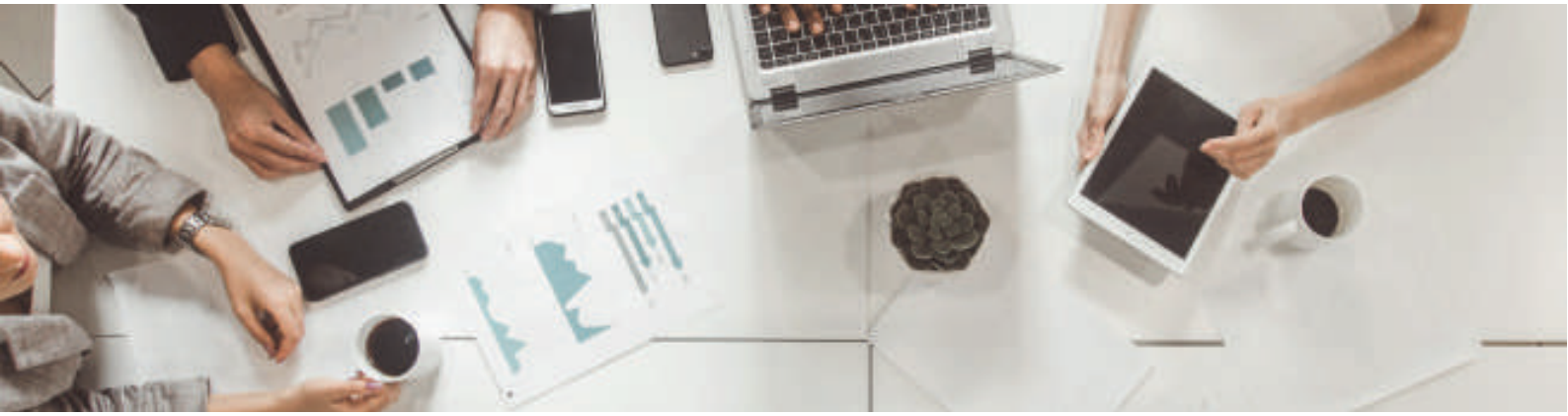
Die Verträge mit Auftragsverarbeitern sollten alle hier aufgeführten Inhalte regeln.

SUBUNTERNEHMER: DAS MÜSSEN SIE BEACHTEN

Dienstleister beschäftigen oft Subunternehmer, an die sie wiederum bestimmte eigene Prozesse auslagern. Die Beauftragung solcher Subunternehmer muss gemäß Art. 28 Abs. 2 DS-GVO vom Verantwortlichen genehmigt werden. Diese Genehmigung ist unabhängig davon einzuholen, ob es bereits einen Vertrag mit dem Auftragsverarbeiter gibt oder nicht. Genehmigt der Verantwortliche die Beschäftigung eines Subunternehmers nicht, so hat der Auftragsverarbeiter diese Weisung zu befolgen und darf den Subunternehmer nicht beschäftigen. Kommt er dieser Weisung nicht nach, muss der Verantwortliche das Auftragsverhältnis beenden.

Die mit dem Auftragsverarbeiter vereinbarten vertraglichen Verpflichtungen müssen ohne Abstriche auch für den Subunternehmer gelten. So muss der Subunternehmer z. B. die gleichen TOM erfüllen wie der Auftragsverarbeiter. Verstößt ein Auftragsverarbeiter gegen diese Pflichten, indem er einen Subunternehmer ohne Genehmigung seitens des Verantwortlichen beauftragt, gilt er dann gemäß Art. 28 Abs. 10 selbst als Verantwortlicher. Hieraus leiten sich direkt rechtliche Folgen wie z. B. die Pflicht zur Erfüllung der Betroffenenrechte und spezielle Haftungsregelungen nach Art. 82 DS-GVO ab. Daraus ergeben

sich auch direkte Schadensersatzforderungen von betroffenen Personen an den Auftragsverarbeiter.



EXKURS: DATENSCHUTZKULTUR

Kaum ein Unternehmen wird seine Datenverarbeitung ohne Unterstützung von Dienstleistern,Auftragsverarbeitern und Subunternehmern durchführen können. Als Datenschutzbeauftragter Ihres Unternehmens stehen Sie in diesem Zusammenhang vor der großen Herausforderung, Ihre internen Datenschutzanforderungen und Sicherheitsvorgaben an diese externen Stellen weiterzugeben.

Letztlich müssen Sie Ihre Dienstleister dazu verpflichten, alle Anforderungen, die sich aus der DS-GVO und sonstigen gesetzlichen Verpflichtungen (Telemediengesetz, Telekommunikationsgesetz usw.) ergeben, erfüllen.

ZUM WOHLE DER BETROFFENEN

Hierzu steht Ihnen ein Instrumentarium an Verträgen, Zertifizierungen, Sicherheitsstandards, nicht zuletzt Checklisten und Seif Assessments zum Nachweis der TOM zur Verfügung. Aber Sie wissen als Datenschutzbeauftragter aus Ihrer täglichen Praxis, dass all das Papier nur dann etwas wert ist, wenn die handelnden Parteien willens sind, sich dieser gemeinsamen Verpflichtung zum Wohle der Betroffenen zu stellen. Das bedeutet aber weitaus mehr als

das bloße Ausfüllen von Checklisten oder das Umsetzen technischer Richtlinien.

VERPFLICHTUNG AUF DEN DATENSCHUTZ

Hier gilt es, in allen beteiligten Unternehmen eine sachgerechte Datenschutzkultur zu etablieren, die sicherstellt, dass alle handelnden Personen sich dem Datenschutz verpflichtet fühlen. Letztlich gilt es Menschen zu überzeugen. Menschen in Ihrem Unternehmen und Menschen bei den jeweiligen Dienstleistern.

MEIN TIPP:

Als Datenschutzbeauftragter sollten Sie sich nicht nur mit den harten vertraglichen oder technischen Fakten einer Auftragsverarbeitung auseinandersetzen. Gehen Sie doch auf Ihre Unternehmensleitung zu und wirken Sie darauf hin, eine Datenschutzleitlinie in Ihrem Unternehmen zu etablieren. Damit kann die Unternehmensleitung nach innen und außen dokumentieren, dass sie sich dem Datenschutz verpflichtet fühlt. Diese Datenschutzleitlinie sollten Sie dann auch Ihren Auftragsverarbeitern zur Verfügung stellen und dort darauf hinwirken, dass deren Unternehmensleitung sich dieser Leitlinie verpflichtet.

Lassen Sie die nachfolgende Datenschutzleitlinie von Ihrer Marketingabteilung in Ihr Unternehmensdesign bringen und im Intranet veröffentlichen.

DATENSCHUTZLEITLINIE

Die folgenden grundlegenden Verhaltensweisen zum Datenschutz manifestieren sich innerhalb unserer Unternehmenskultur auf der organisatorischen und persönlichen Ebene. Diese Verhaltensweisen werden durch Ethik, Kultur oder Einstellung im Unternehmen aber auch in gleichem Maße auf der individuellen Ebene jedes Einzelnen bestimmt.

Verhalten	Organisatorische Ebene	Individuelle Ebene
1. Datenschutz ist Teil der täglichen Arbeit und Teil des rechtskonformen Lebens.	Das Verhalten weist darauf hin, dass der Datenschutz als Geschäftszweck bei der Festlegung von Organisationszielen akzeptiert wird.	Der Einzelne kümmert sich um das Wohlergehen des Unternehmens und das von Personen, deren personenbezogenen Daten verarbeitet werden. Der Einzelne wendet bei seiner täglichen Arbeit Datenschutztechniken an und kann die Datenschutzgrundsätze umsetzen.
2. Die Menschen respektieren die Wichtigkeit von Datenschutzrichtlinien und -grundsätzen.	Datenschutzrichtlinien und Prinzipien werden von der Geschäftsleitung eindeutig befürwortet. Die Genehmigung, Überprüfung und Kommunikation von Richtlinien findet regelmäßig statt.	Die Beschäftigten haben die Datenschutzrichtlinien gelesen und verstanden, haben Datenschutzschulungen und fortlaufende Sensibilisierungsmaßnahmen erhalten und fühlen sich dazu befähigt, die Datenschutzrichtlinien des Unternehmens zu befolgen.
3. Die Menschen erhalten eine ausreichende und detaillierte Anleitung zum Datenschutz und werden ermutigt, sich an der aktuellen Situation des Datenschutzmanagements zu beteiligen und diese zu hinterfragen.	Ein wechselseitiger Kommunikationsprozess für Beratung und Feedback bietet Stakeholdern die Möglichkeit, Änderungen zu kommentieren.	Stakeholder demonstrieren Partizipation. Sie hinterfragen Datenschutzpraktiken, zeigen Datenschutzprobleme auf und liefern auf Anfrage Hinweise zu Verbesserungen.
4. Jeder ist verantwortlich für den Schutz von Informationen innerhalb des Unternehmens.	Sind bei bestimmten Angelegenheiten Disziplin und Sanktionen erforderlich, werden diese umgesetzt und von den Stakeholdern bestätigt.	Jeder Einzelne muss seinen Verantwortlichkeiten bezüglich der Einhaltung der Datenschutzrichtlinien und der Datenschutzgrundsätze verstehen.

5. Stakeholder sind sich bewusst, wie sie Bedrohungen für das Unternehmen erkennen und darauf reagieren können.	Angemessene Prozesse zur Erkennung und Reaktion auf Bedrohungen der Privatsphäre und Datenschutzverletzungen können durch einen wirksamen Reporting-Prozess und ein Verfahren zur Reaktion auf Sicherheitsverletzungen implementiert werden, um Risiken zu minimieren.	Die Menschen müssen über alle Arten von Datenschutzverletzungen aufgeklärt werden und darüber, wie man sie melden und darauf reagieren kann.
6. Das Management unterstützt und antizipiert aktiv neue Datenschutz-Innovationen und kommuniziert diese an das Unternehmen. Das Unternehmen ist offen dafür, neue Herausforderungen der Informationssicherheit zu erkennen und zu bewältigen.	Datenschutz-Innovationen und -Herausforderungen werden durch ein Team von Spezialisten für Datenschutzmanagement angegangen.	Die Datenschutzkultur trägt dazu bei, dass Stakeholder neue Ideen vorantreiben.
7. Das Management engagiert sich in kontinuierlicher funktionsübergreifender Zusammenarbeit, um effiziente und effektive Datenschutzprogramme zu etablieren.	Die funktionsübergreifende Zusammenarbeit wird durch die organisatorische Akzeptanz einer ganzheitlichen Strategie für das Datenschutzmanagement und die verbesserte Integration des Schutzes der Privatsphäre in das Unternehmen gestärkt.	Der Einzelne erkennt auch in anderen Organisationseinheiten Risiken und Datenschutzverletzungen und identifiziert Verbesserungspotenziale sowie potenzielle Synergien zur Etablierung neuer Datenschutzmaßnahmen.

8. Die Geschäftsleitung erkennt den geschäftlichen Wert der Privatsphäre an.	Der geschäftliche Wert des Datenschutzes wird auf organisatorischer Ebene erkannt, wenn der Datenschutz als Mittel betrachtet wird, um den Geschäftswert (Einnahmen, Ausgaben, Reputation und Wettbewerbsvorteil) zu verbessern, das Vertrauen der Kunden zu erhalten und den Markenwert zu verbessern. Transparenz bei der Reaktion auf Verletzungen des Datenschutzes ist hierbei der Schlüssel.	Das Verhalten wird durch die Generierung kreativer Ideen zur Verbesserung des Nutzwerts (verschiedene Aktivitäten zum Schutz der Privatsphäre) belegt.

Diese Datenschutzleitlinie basiert auf einer Veröffentlichung der „ Information Systems Audit and Control Association" (ISACA).

TOM: Diese Maßnahmen müssen Sie fordern

Die meisten Anforderungen aus der DS-GVO an den technischen Datenschutz - nämlich Datenminimierung, Datenschutz durch Technikgestaltung und Umsetzung technischer und organisatorischer Maßnahmen - sind grundsätzlich bereits aus dem BDSG (alt) bekannt. So fordert der § 3a BDSG (alt) bereits „so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen". Auch „die Auswahl und Gestaltung von Datenverarbeitungssystemen" hat sich an diesem Ziel auszurichten. Die Anforderung an die verantwortliche Stelle und einen etwaigen Auftragnehmer, geeignete

technische und organisatorische Maßnahmen zu treffen, ist in § 9 BDSG (alt) nebst Anlage zu § 9 vorhanden. Die Forderung des Art. 25 Abs. 2 - Datenschutz durch datenschutzfreundliche Voreinstellung - ist dagegen nicht ausdrücklich im BDSG (alt) enthalten. Erwägungsgrund 78 der EU-DS-GVO spricht davon, dass Hersteller von Produkten, Diensten und Anwendungen „ermutigt werden“ sollen, den Datenschutz bereits „bei der Entwicklung und Gestaltung ihrer Produkte, Dienste und Anwendungen zu berücksichtigen.“

Die nachfolgenden Schutzziele sind in der DS-GVO explizit aufgeführt:

ÜBERSICHT: SCHUTZZIELE

Schutzziel	Fundstelle DS-GVO
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben	Art. 5 Abs. 1 lit. a
Transparenz	Art. 5 Abs. 1 lit. a, Art. 13 und Art. 14
Zweckbindung	Art. 5 Abs. 1 lit. b
Datenminimierung	Art. 5 Abs. 1 lit. c
Speicherbegrenzung (Erforderlichkeitsgebot)	Art. 5 Abs. 1 lit. e
Richtigkeit	Art. 5 Abs. 1 lit. d
Integrität	Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. b
Vertraulichkeit	Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. b
Verfügbarkeit und Belastbarkeit beim Betrieb	Art. 32 Abs. 1 lit. b
Verfügbarkeit bei einem physischen oder technischen Zwischenfall	Art. 32 Abs. 1 lit. c

Keine Zeit für Datenschutz neben Ihrem Kerngeschäft?

Sie haben neben Ihrem Kerngeschäft keine Zeit für lästigen Datenschutz? Sie wissen nicht, was Sie genau dokumentieren müssen und wo Sie anfangen sollen? Kein Problem!

Wir helfen Ihnen **schnell und ohne großen Aufwand DSGVO-konform** zu werden und den Aufsichtsbehörden selbstbewusst entgegen zu treten. **Alle Informationen**, die Sie als Kleinunternehmer und Startup zur DSGVO wissen müssen. **Vorgefertigte Muster**, bei denen Sie nur Ihre persönlichen Daten einfüllen müssen. Alles in einem Paket und **auf einem Blick.**

Datenschutz Starterkit für KMU und Startups- schnell und einfach DSGVO-konform!

Keine Bange, wenn Sie bislang noch nichts getan haben. Wir helfen Ihnen, **schnell und unkompliziert** die Datenschutzbestimmungen anzuwenden!

Das **Datenschutz-Starterkit** ist speziell für Kleinunternehmer und Startups entwickelt und auf Ihre Datenschutz-Anforderungen angepasst. Lesen Sie nur das, was wirklich wichtig ist.

Das Starterkit enthält:

- **Praxisleitfaden inkl. Schritt-für-Schritt Anleitung** zum datenschutzkonformen Unternehmen und Antworten auf die häufigsten Fragen der Aufsichtsbehörden
- **USB-Stick** mit allen wichtigen **Musterverträgen** und Vorlagen im Word-Format: Sie müssen nur noch Ihre persönlichen Informationen eingeben!
- **Mitarbeiterinformationen zum Datenschutz:** Sie sind auch verantwortlich Ihre Mitarbeiter zum Datenschutz aufzuklären. Verteilen Sie einfach die beiliegende Mitarbeiterinformationsbroschüre an Ihre Mitarbeiter!

Jetzt das Datenschutz Starterkit bestellen! »

Während Verstöße gegen die §§ 3a und 9 (nebst Anlage zu § 9) BDSG-alt für sich genommen bisher keinen bußgeldbewehrten Tatbestand darstellen, sind Verstöße gegen die Artt. 25 und 32 DS-GVO mit einem Bußgeld der Kategorie 10 Mio. €/2 % des weltweiten Jahresumsatzes eines Unternehmens bedroht. Verstö ße gegen Art. 5 DS-GVO sind gar mit einem Bußgeld der Katego rie 20 Mio. €/4 % des weltweiten Jahresumsatzes eines Unter nehmens bedroht.

Mythos und Wahrheit: Kennen Sie sich mit der Auftrags-verarbeitung aus?

Werden personenbezogene Daten verarbeitet und bedient sich Ihr Unternehmen dabei Dienstleistern (z.B. IT-Dienstleistern), spielt die Frage eine besonders wichtige Rolle, ob es sich dabei um eine Auftragsverarbeitung handelt. Dabei kann es notwendig sein, dass Sie - beispielsweise im Rahmen einer Beratung - mit einigen Mythen aufräumen.

MYTHOS 1: DER VERANTWORTLICHE ENTSCHEIDET ALLEIN ÜBER DIE INHALTE EINES VERTRAGS ZUR AUFTRAGS VERARBEITUNG

Die Wahrheit ist: Ähnlich wie § 11 des alten Bundesdatenschutz gesetzes (BDSG-alt) gibt Art. 28 Datenschutz-Grundverordnung (DS-GVO) nur die Rahmenbedingungen der Auftragsverarbeitung vor. So ergibt sich aus Art. 28 Abs. 3 DS-GVO, welcher Inhalt zwischen Verantwortlichem und Auftragsverarbeiter zu vereinbaren ist. Dabei handelt es sich im Wesentlichen um„ Überschriften››. Konkrete Regelungen müssen Verantwortlicher und Auftragsverarbeiter festlegen. Dabei kann festlegen auch bedeuten, dass beide Parteien die Inhalte aushandeln. Das ist grundsätzlich zulässig. Der Auftragsverarbeiter kann bei der Festlegung mitreden und ist nicht gezwungen, die Forderungen des Verantwortlichen zu akzeptieren. Das meiste ist verhandelbar.

MYTHOS 2: ES MUSS VOM AUFTRAGSVERARBEITER DER VOM AUFTRAGGEBER VORGEGEBENE VERTRAG AKZEPTIERT WERDEN

Die Wahrheit ist: In erster Linie handelt es sich bei der Vereinbarung zur Auftragsverarbeitung um einen ganz normalen Vertrag. Weil die meisten Inhalte Verhandlungssache sind, kann auch der Auftragsverarbeiter bei der Formulierung der Inhalte mitreden. Manchmal ist das jedoch graue Theorie. Sind Verantwortlicher oder Auftragsverarbeiter in einer schlechten Verhandlungsposition, etwa weil sie auf den anderen angewiesen sind, kann der Vertragspartner mit der größeren Verhandlungsmacht die Regeln „diktieren“. Der Schwächere muss dann die Regeln akzeptieren, will er den Partner nicht verlieren. Hier wird deutlich, dass nicht nur der Datenschutz eine Rolle spielen kann, sondern vor allem wirtschaftliche Aspekte.

MYTHOS 3: VOR DEM 25.5.2018 GESCHLOSSENE VERTRÄGE ZUR AUFTRAGSDATENVERARBEITUNG SIND NICHT MEHR GÜLTIG

Die Wahrheit ist: Auch bei Vereinbarungen zur Auftragsverarbeitung handelt es sich um Verträge. Diese Regelungen von Rechten und Pflichten werden

nicht dadurch hinfällig, dass sich gesetzliche Rahmenbedingungen ändern. Grundsätzlich gelten auch in einem solchen Fall geschlossene Verträge weiter. Allerdings müssen alte Verträge ggf. ausgelegt werden, sprich, es muss danach gefragt werden, was die Parteien regeln wollten. Dabei sollten Sie stets berücksichtigen: Vergleichen Sie § 11 BDSG-alt und Art. 28 DSGVO, sind die Festlegungen im Wesentlichen deckungsgleich?

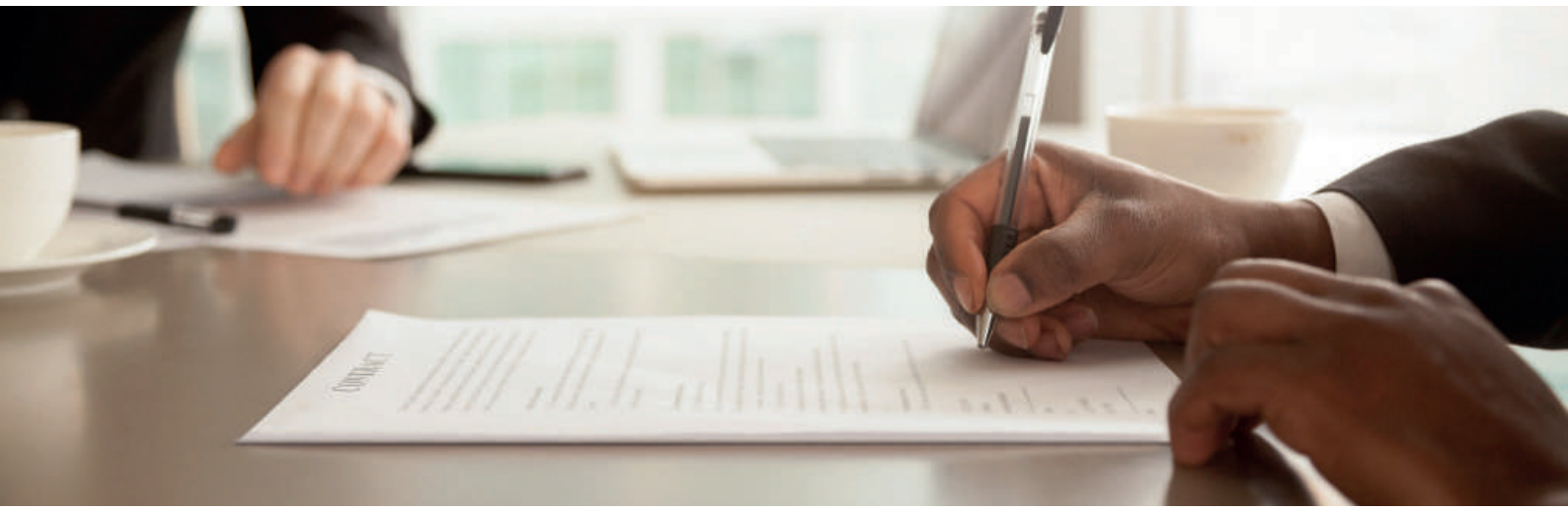
MYTHOS 4: ES MUSS EINEN VERTRAG MIT 2 UNTERSCHRIFTEN AUF DEM DOKUMENT GEBEN

Die Wahrheit ist: Im Allgemeinen ist das richtig. Allerdings heißt es, genau hinzuschauen, und zwar in § 126 Abs. 2 Bürgerliches Gesetzbuch (BGB). Dort ist festgelegt, dass zwar bei einem Vertrag grundsätzlich die Unterzeichnung der Parteien auf derselben Urkunde erfolgen muss. Gibt es von einem Vertrag mehrere gleich lautende Urkunden, sprich für jede Partei einen Ausdruck des Vertrags, so reicht es aber aus, wenn jede Partei die für die andere Partei bestimmte Urkunde unterzeichnet.

Hinweis: Selbst die Schriftform Ist bei einer Auftragsverarbeitung nicht zwingend vorgeschrieben. Auch ein elektronisches Format kann zulässig sein (Art. 28 Abs. 9 DSGVO). Das könnte beispielsweise ein Vertrag im PDF-Format sein, der von den Parteien signiert wird. Doch Letzteres unterliegt wieder besonderen Anforderungen, wenn man eine Signatur nach dem Signaturgesetz fordert, welche die Schriftform ersetzen kann (§§ 126 Abs. 3, 126a BGB).

MYTHOS 5: DER DATENSCHUTZBEAUFTRAGTE MUSS AUFTRAGSVERARBEITUNGSVERTRÄGE ABSCHLIESSEN

Die Wahrheit ist: Heute wie früher sind Sie in erster Linie der Berater Ihres Unternehmens in Datenschutzfragen. Wer schlussendlich die Entscheidungen zur Umsetzung des Datenschutzes trifft, liegt eigentlich klar auf der Hand: der Verantwortliche, sprich Ihre Unternehmensleitung. Sie können daher bei der Erstellung, Prüfung und sogar Verhandlung von Auftragsverarbeitungs-



verträgen unterstützen, wenn Sie über das notwendige Wissen verfügen. Außerdem wichtig: Sie vertreten nicht das Unternehmen. Daher brauchen Sie die Vereinbarungen nicht unterzeichnen. Im Gegen teil: Sie könnten ein Haftungsproblem bekommen, wenn Sie Festlegungen akzeptieren, beispielsweise zu den Schutzmaßnahmen, die nicht oder anders umgesetzt sind.

MYTHOS 6: ES BEDARF KEINER RECHTSGRUNDLAGE, WENN EIN FALL DER AUFTRAGSVERARBEITUNG GEGEBEN IST

Die Wahrheit ist: Das trifft leider überhaupt nicht zu. Generell be darf es für jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage (vgl. Art. 6 Abs. 1 DS-GVO). Werden Dienstleister eingebunden und verarbeiten diese personenbezogenen Daten auf Weisung des Verantwortlichen, liegt ein Fall der Auftragsverarbeitung vor. In diesem Fall müssen die Rahmenbedingungen des Art. 28 DS-GVO eingehalten werden. Das hat mit dem Vorliegen einer Rechtsgrundlage nichts zu tun.

Impressum

Angaben gemäß § 5 TMG

mediaforwork, ein Unternehmensbereich der

VNR Verlag für die Deutsche Wirtschaft AG

Theodor-Heuss-Straße 2-4

D-53177 Bonn

Großkundenpostleitzahl: D-53095 Bonn

Handelsregister: HRB 8165

Registergericht: Amtsgericht Bonn

Vertreten durch den Vorstand:

Richard Rentrop

Kontakt

Telefon: 0228 - 9 55 01 20 (Kundendienst)

Telefax: 0228 - 36 96 480

E-Mail: kundendienst@wirtschaftswissen.de

Internet: https://www.wirtschaftswissen.de/

Umsatzsteuer

Umsatzsteuer-Identifikationsnummer gemäß §27 a Umsatzsteuergesetz:

DE 812639372

Verantwortlich für den Inhalt nach § 55 Abs. 2 RStV

Michael Jodda

Theodor-Heuss-Straße 2-4

D-53177 Bonn

Streitschlichtung

Die Europäische Kommission stellt eine Plattform zur Online-Streitbeilegung (OS) bereit: https://ec.europa.eu/consumers/odr.

Unsere E-Mail-Adresse finden Sie oben im Impressum.
Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Haftung für Inhalte

Als Diensteanbieter sind wir gemäß § 7 Abs.1 TMG für eigene Inhalte auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich. Nach §§ 8 bis 10 TMG sind wir als Diensteanbieter jedoch nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Haftung für Links

Unser Angebot enthält Links zu externen Websites Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar.

Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Urheberrecht

Die durch die Seitenbetreiber erstellten Inhalte und Werke auf diesen Seiten unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechtes bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Downloads und Kopien dieser Seite sind nur für den privaten, nicht kommerziellen Gebrauch gestattet.

Soweit die Inhalte auf dieser Seite nicht vom Betreiber erstellt wurden, werden die Urheberrechte Dritter beachtet. Insbesondere werden Inhalte Dritter als solche gekennzeichnet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir um einen entsprechenden Hinweis. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Inhalte umgehend entfernen.

Bildnachweis

Adobe Stock, https://stock.adobe.com/de/

© VNR Verlag für die Deutsche Wirtschaft AG