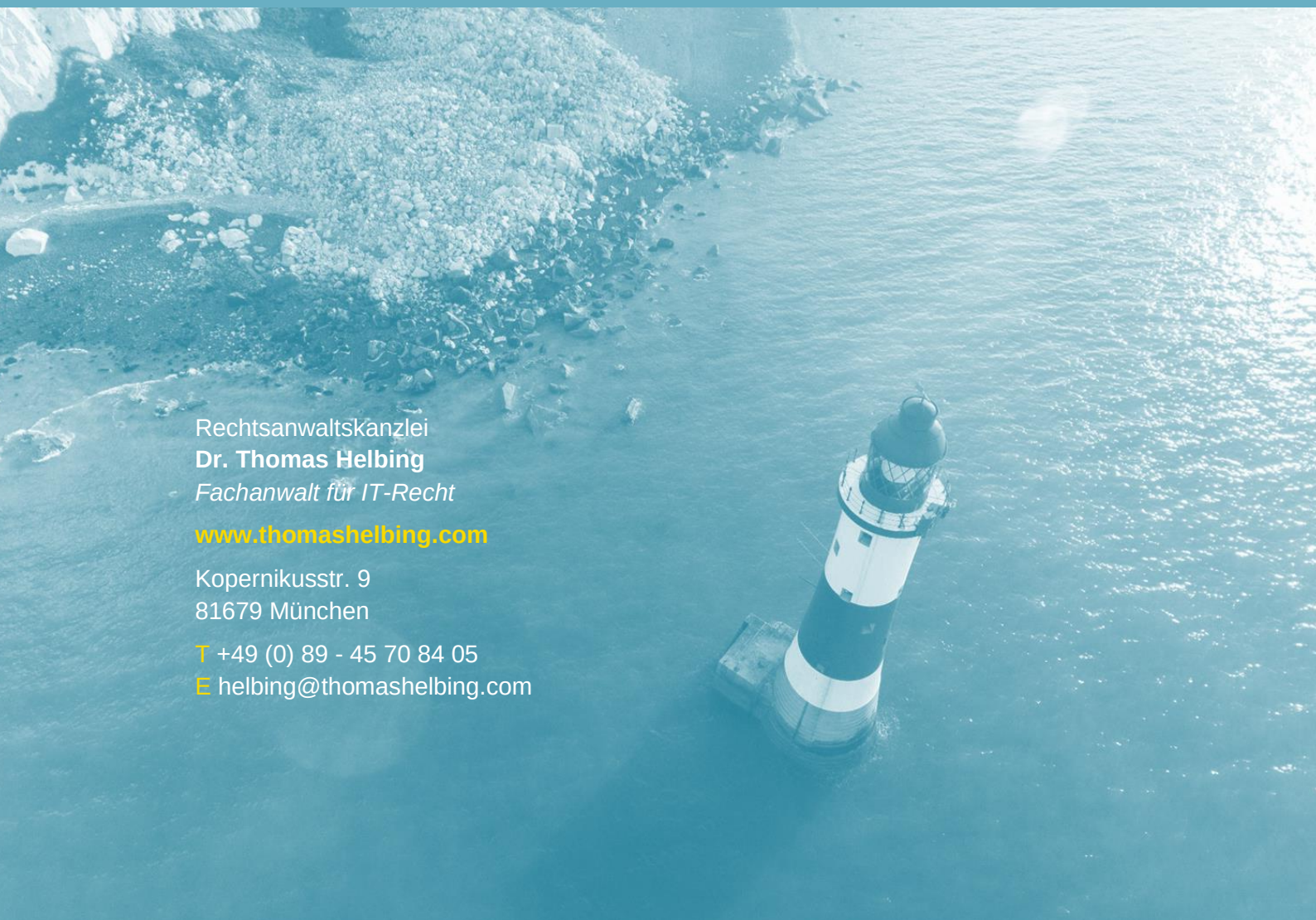
HELBING
Kanzlei für IT- und Datenschutzrecht

PRAXISLEITFADEN

DSGVO FÜR IT-DIENSTLEISTER

DIE DATENSCHUTZGRUNDVERORDNUNG UMSETZEN ALS AUFTRAGSVERARBEITER

Erläuterungen, Beispiele und Checklisten



Rechtsanwaltskanzlei
Dr. Thomas Helbing
Fachanwalt für IT-Recht
www.thomashelbing.com
Kopernikusstr. 9
81679 München
T +49 (0) 89 - 45 70 84 05
E helbing@thomashelbing.com

EINLEITUNG

Sie bieten „Software as a Service“, Hosting-, Cloud- oder vergleichbare Leistungen für Unternehmen an?

Sie entwickeln und betreiben für Unternehmen Webseiten, Apps oder andere Online-Plattformen?

Sie speichern dabei Daten zu den Endkunden, Mitarbeitern oder Nutzern ihrer Kunden oder haben auf solche Daten Zugriff?

Dann sind Sie ein sogenannter „Auftragsverarbeiter“, für die ab 25. Mai 2018 mit der Datenschutzgrundverordnung (DSGVO) neue, spezielle Regeln gelten.

Es besteht Handlungsbedarf, um

- gute Kunden zu behalten und neue zu gewinnen
- Haftungsrisiken zu minimieren, und
- Bußgelder zu vermeiden
  (theoretisch bis 20 Mio. Euro oder 4 % des weltweiten Umsatzes).

Die Datenschutzgrundverordnung bringt für alle Unternehmen in der EU erhebliche Neuerungen und führt zu intensiven Anstrengungen bei Unternehmen, um sich auf die neuen Datenschutzregeln vorzubereiten. Für Auftragsverarbeiter ergeben sich ganz spezifische Änderungen: Ihre datenschutzrechtliche Verantwortung steigt, neue Kunden-Verträge werden nötig, das Haftungsrisiko erhöht sich und es gelten erweiterte Dokumentationspflichten.

Der folgende Beitrag erläutert praxisnah und anhand von Beispielen welche konkreten Schritte Sie unternehmen müssen, um als Auftragsverarbeiter der Datenschutzgrundverordnung gerecht zu werden.

Zur Umsetzung der Anforderungen der DSGVO können Sie ein Rechtspaket mit Checklisten, Mustern und Vorlagen bestellen (DSGVO-Kit). Einzelheiten dazu finden Sie am Ende des Beitrags sowie online unter www.complyvacy.com/dsgvo-kit.

München, April 2018

Dr. Thomas Helbing
Fachanwalt für IT-Recht

BIN ICH ÜBERHAUPT AUFTRAGSVERARBEITER?

Auftragsverarbeiter im Sinne der Datenschutzgrundverordnung sind alle, die für andere „personenbezogene Daten im Auftrag“ verarbeiten, Art. 4 Nr. 8 DSGVO.

Typische Fälle sind:

- Anbieter web-basierter Softwarelösungen (“Software as a Service“), in der Kunden personenbezogene Daten speichern

  Beispiele SaaS: Software für das „Customer Relationship Management“ (CRM-Systeme), Online Shops, Newsletter und Online-Marketing Software, Bewerbermanagement-Tools, HR-Software, Web-Tracking Anbieter, Online Software für das Projektmanagement oder die Zeiterfassung, Anwendungen im Bereich Fakturierung und Finanzbuchhaltung oder webbasierte ERP-Systeme.

- Unternehmen, die für ihre Kunden Backend-Dienste für mobile Apps betreiben und darin Nutzerdaten erfassen

  Speicherung der E-Mail Adresse und Einstellungen von App-Nutzern in einem Backend

- Online-Agenturen, die auch das Hosting oder den Betrieb von Webseiten übernehmen, wenn diese personenbezogene Daten beinhalten

  Betrieb und Wartung einer Webseite mit Kontaktformular oder Newsletter-Bestellfunktion.

- Sonstige IT-Dienstleister, zu deren Leistungen der Umgang mit personenbezogenen Kundendaten gehört

  z.B. Datenkonvertierungen, Import von Kundendaten in ein ERP-System, Analyse und Auswertung von Kundendaten

- Shared Service Center für IT-Dienste im Konzern

  z.B. eine IT-Tochtergesellschaft bietet IT-Dienstleistungen für alle Konzernunternehmen an und verarbeitet dabei die Daten derer Mitarbeiter.

Der Begriff der „personenbezogenen Daten“ umfasst alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, so die Definition in Art. 4 Nr. 1 DSGVO. Auf die Sensibilität der Daten kommt es nicht an. Die bloße Information, dass eine Person bei einem Unternehmen angestellt ist, dort einen Newsletter bestellt oder Produkte gekauft hat, stellt also bereits ein personenbezogenes Datum dar. Personenbezogen Daten müssen zudem nicht unbedingt Namen enthalten. Es genügt wenn die Daten einer natürlichen Person zugeordnet werden können. Wenn die Datensätze E-Mail Adressen oder IP-Adressen enthalten ist häufig die Personenbeziehbarkeit bereits gegeben.

Missverstanden wird oft auch der der Ausdruck „verarbeiten“. Eine Verarbeitung ist letztlich jeder Umgang mit personenbezogenen Daten. Die DSGVO nennt als Beispiele (Art. 4 Nr. 2 DSGVO): Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten. Ein Anbieter von Cloudspeicher, bei dem Kunden personenbezogene Daten ablegen „verarbeitet“ diese also bereits.

Eine Verarbeitung „im Auftrag“ liegt immer vor, wenn der Kunde das „Wieso“ bzw. „Warum“ und das wesentliche „Wie“ der Verarbeitung festlegt. Dabei kann dem Auftragsverarbeiter durchaus ein gewisser Spielraum eingeräumt werden, etwa in Bezug auf die Datensicherheitsmaßnahmen. Grundsätzlich kann man sagen, dass nach der DSGVO der Anwendungsbereich der Auftragsverarbeitung gegenüber dem BDSG-1990 weiter gefasst ist. In den oben genannten Beispielsfällen liegt eine Auftragsverarbeitung vor. Grenzfälle entstehen dann, wenn der Auftragnehmer weitgehende Entscheidungsbefugnisse erhält.

Ein Unternehmen, das eine Bewerbermanagement-Software bereitstellt, verarbeitet

die Bewerberdaten im Auftrag. Ein Unternehmen, das für andere vollständig die Recruiting-Funktion übernimmt und selbst festlegt, welche Kandidaten wie und in welcher Form angesprochen werden und welche Software dabei genutzt wird, verarbeitet die Daten dagegen nicht mehr im Auftrag, sondern wird selbst datenschutzrechtlich zum „Verantwortlichen".

HINTERGRUND: RECHTSTEXTE

Ab 25. Mai 2018 gilt mit der EU-Datenschutzgrundverordnung 2016/679 (DSGVO) ein reformiertes Datenschutzrecht in Europa. Als Verordnung gilt die DSGVO unmittelbar in ganz Europa.

Bisher war das Datenschutzrecht in Europa hauptsächlich in der EU Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 geregelt. Eine Richtlinie gilt nicht direkt für Unternehmen, sondern verpflichtet die Mitgliedstaaten, nationale Gesetze zu erlassen, um die Vorgaben verbindlich zu machen. Deutschland hat die Datenschutzrichtlinie vor allem durch das Bundesdatenschutzgesetz (BDSG-1990) umgesetzt.

Die DSGVO erlaubt den EU Mitgliedstaaten nur noch in engen Grenzen eigene Datenschutzgesetze zu erlassen, etwa für Mitarbeiterdaten. Deutschland hat von dieser Möglichkeit Gebrauch gemacht und ein komplett neues Bundesdatenschutzgesetz (BDSG-2018) erlassen, das wie die DSGVO am 25. Mai 2018 in Kraft tritt. Ab diesem Datum müssen sich Unternehmen also an die DSGVO halten und ergänzend auch das BDSG-2018 beachten.

Das Datenschutzrecht ist daneben auf europäischer und nationaler Ebene noch in einer Vielzahl weiterer Bestimmungen geregelt, die sich etwa auf die Telekommunikation, auf Online-Dienste und den Sozialbereich beziehen. Diese Bestimmungen werden oder müssen im Rahmen der Neuerungen der DSGVO teilweise noch angepasst werden, was zu einer komplexen Gemengelage führt. Im Online-Bereich ist ebenfalls eine neue Verordnung, die ePrivacy-Verordnung in der Entstehung.

TO-DO 1:

Datenschutzverträge mit Kunden abschließen bzw. überarbeiten

DSGVO-konforme Auftragsverarbeitungsverträge mit Kunden abschließen und alte überarbeiten.

Mustervertrag entwickeln, der der DSGVO und Ihren individuellen Anforderungen gerecht wird.

Auftragsverarbeitungsverträge, die von Kunden vorgelegt werden nicht sorglos unterschreiben, sondern prüfen.

DATENSCHUTZVERTRÄGE MIT KUNDEN ABSCHLIEßEN BZW. ÜBERARBEITEN

Schon das aktuelle Recht verlangt, dass Sie als Auftragsverarbeiter mit ihren Kunden spezielle Datenschutzverträge schließen. Die Verträge werden als „Auftragsdatenverarbeitungsverträge“ (kurz ADV-Verträge) bezeichnet. Dies ist bisher in § 11 Bundesdatenschutzgesetz (BDSG-1990) geregelt. Die Verträge müssen schriftlich geschlossen werden, ein Online-Abschluss genügt unter Geltung des BDSG-1990 nicht. Die DSGVO bringt hier die Erleichterung, dass auch ein elektronischer Vertragsschluss möglich ist.

Viele Unternehmen haben solche Verträge bisher nicht unterzeichnet. Die Pflicht zum Abschluss lag bisher in erster Linie bei den Auftraggebern, also Ihren Kunden, und nicht bei Ihnen als Auftragsverarbeiter.

Die DSGVO verpflichtet nunmehr aber auch Auftragsverarbeiter zum Abschluss von Verträgen zur Auftragsverarbeitung, Art. 28 Abs. 3 DSGVO. Bei Verstößen drohen nach der DSGVO dem Auftragsverarbeiter Bußgelder von bis zu € 10.000.000. Bei Unternehmen sind sogar Bußgelder bis 2 % des weltweiten Jahresumsatzes möglich, wenn dieser Betrag höher ist. Auch wenn in der Praxis die Bußgelder kaum solche Höhen erreichen dürften, bereits unter dem BDSG-1990 haben Datenschutzbehörden für mangelhafte Verträge Bußgelder von über 10.000 € verhängt.

Als Auftragsverarbeiter müssen Sie also mit allen Kunden, deren personenbezogene Daten Sie im Auftrag verarbeiten, einen solchen speziellen Vertrag schließen. Aufgrund der DSGVO ist bei vielen Unternehmen das Thema Datenschutz in den Fokus geraten. Es ist daher zu erwarten, dass auch ihre Kunden zukünftig stärker rechtskonforme Datenschutzverträge einfordern werden.

Dies gilt übrigens nicht nur für Ihre Kunden in der EU. Die DSGVO gilt auch für Unternehmen außerhalb der EU, wenn diese z.B. Produkte und Leistungen an Personen in der EU anbieten (z.B. ein US Unternehmen bietet seine App auch im deutschen App-Store an). Diese „exterritoriale Geltung“ in der DSGVO ist gegenüber dem BDSG-1990 neu.

Wer mit seinen Kunden bereits Auftragsdatenverarbeitungsverträge gemäß dem BSDG-1990 geschlossen hat, sollte diese durch neue Verträge ersetzen, die speziell auf die DSGVO zugeschnitten sind. Zwar sind die Anforderungen der DSGVO gegenüber dem BDSG-1990 ähnlich, es gibt jedoch wichtige Unterschiede. Einige davon finden Sie nachfolgend beispielhaft erläutert:

Einschaltung von Unterauftragnehmern.

Bereits das BDSG-1990 verlangt, dass in dem Auftragsdatenverarbeitungsvertrag geregelt ist, unter welchen Voraussetzungen Unterauftragnehmer eingeschaltet werden dürfen, § 11 Abs.2 Nr. 6 BDSG-1990. Die DSGVO verlangt nunmehr, dass vor Einschaltung eines Unterauftragnehmers der Auftraggeber dies genehmigen muss. Der Auftraggeber kann zwar eine weitreichende Generaleinwilligung geben, in diesem Falle muss der Auftragsverarbeiter aber vor jeder Änderung bei Unterauftragnehmern den Auftraggeber informieren und der Auftraggeber kann der Änderung widersprechen! (Art. 28 Abs. 2, Abs. 3 Satz 2 Buchstabe d) DSGVO).

Sie bieten Unternehmen eine Reisekostenabrechnung als Online-Software an (Software as a Service) und nutzen hierfür Hosting oder Cloud-Dienstleistungen von Amazon, Azure oder eines sonstigen Hosters. Der Hoster ist rechtlich betrachtet ihr Unterauftragnehmer. Sie müssen sich im Auftragsverarbeitungsvertrag mit dem Kunden diesen genehmigen lassen. Zwar können Sie sich eine Generaleinwilligung für den Einsatz eines beliebigen Hosters geben lassen. Wenn Sie den Hoster später wechseln, müssen Sie aber den Kunden informieren und dieser kann widersprechen. Das könnten Kunden nutzen, um sich vom Vertrag vorzeitig zu lösen. Außerdem dürften Sie in technische Schwierigkeiten kommen, wenn Sie bestimmte Kunden nicht auf den neuen Hoster umziehen dürfen. Sie sollten daher vertraglich genau regeln, wie die Einschaltung von Unterauftragnehmern aussieht, z.B. festlegen, dass auch Sie dem Kun-

den kundigen können, wenn dieser grundlos einen neuen Hoster ablehnt.

Pflicht zur Unterstützung des Auftraggebers

In dem Auftragsverarbeitungsvertrag müssen Sie sich verpflichten, ihren Kunden bei der Erfüllung von bestimmten Pflichten des Kunden gemäß der DSGVO zu unterstützen, Art. 28 Abs. 3 Satz 2 Buchstabe e) und f) DSGVO.

Ihr Kunde ist nach der DSGVO zum Beispiel verpflichtet, den Personen, über die er Daten speichert, auf Anforderung eine Kopie sämtlicher gespeicherten Daten bereitzustellen, Art. 15 Abs. 3 DSGVO. In bestimmten Fällen können die Betroffenen gemäß der DSGVO sogar verlangen, dass ihnen die Daten in einem „gängigen, maschinenlesbaren Format" (z.B. als CSV Datei) bereitgestellt werden (sogenanntes „Recht auf Datenübertragbarkeit", Art. 20 DSGO). Daneben müssen ihre Kunden ab 25. Mai 2018 bei bestimmten sensiblen Datennutzungen aufwändige Datenschutzprüfungen, sog. Datenschutzfolgeabschätzungen, vornehmen, Art. 35 DSGVO.

Bei all diesen Pflichten müssen Sie als Auftragsverarbeiter den Kunden ggf. unterstützen, so verlangt es das Gesetz. Sie sollten daher vertraglich festlegen, wie weit ihre Pflichten gehen, etwa ob eine von Ihnen angebotene Software Funktionen zum Datenexport bereitstellen muss und, dass etwaige Unterstützungsleistungen gesondert zu vergüten sind.

Haftung

Unter der DSGVO erhöht sich ihr Haftungsrisiko als Auftragsverarbeiter gegenüber dem BDSG-1990. So verpflichtet die DSGVO ausdrücklich sowohl den Auftraggeber als *auch* den Auftragsverarbeiter angemessene Maßnahmen zur Datensicherheit zu treffen, Art. 32 DSGVO. Bei Verstößen drohen Bußgelder, auch das ist im Bereich der Datensicherheit neu. Kommt es zu einer Datenpanne können die Personen, deren Daten Sie für Ihre Kunden speichern, direkt Sie als Auftragsverarbeiter in Anspruch nehmen, Art. 82 Abs. 1, 2 DSGVO. Sie sitzen mit dem Kunden quasi haftungsrechtlich in einem Boot, Art. 82 Abs. 4 DSGVO. Sie können Ansprüche der Betroffenen nur abwehren oder bei Ihrem Kunden Regress nehmen, wenn Sie nachweisen, dass Sie an dem Schaden keine Verantwortung trifft. Diese Haftungsregelung verschärft sich dadurch, dass Betroffene unter der DSGVO, anders als nach bisherigem Recht, auch Ersatz von immateriellen Schäden (z.B. Rufschädigung, Verletzung des Persönlichkeitsrechts) geltend machen können, Art. 82 Abs. 1 DSGVO und ihre Ansprüche am eigenen Wohnsitz oder Aufenthaltsort (ggf. im EU-Ausland) einklagen können, Art. 79 Abs. 2 SDGVO.

Sie entwickeln und betreiben für Ihre Kunden Online-Shops und nutzen hierfür ein Open-Source Tool (z.B. Magento, Wordpress, Drupal), für das Sie selbst branchenspezifische Erweiterungen programmiert haben. Aufgrund einer Sicherheitslücke in der Open-Source Software konnten Angreifer Bestelldaten von Endkunden erlangen. Die Betroffenen eines kleinen Online-Shops verlangen von Ihnen Schadenersatz. Der Kunde hatte Sie nicht explizit mit dem Einspielen von Sicherheits-Updates oder der Sicherheitsprüfung von Standardkomponenten des Open-Source Tools beauftragt.

Vor dem Hintergrund der Haftungsrisiken gerade im Bereich der Datensicherheit müssen in Auftragsverarbeitungsverträgen explizite Regelungen zu den Verantwortungsbereichen bei der Datensicherheit geregelt werden. Außerdem empfehlen sich Haftungsregelungen, die das Innenverhältnis zwischen Ihnen und dem Kunden bei Ansprüchen von Betroffenen regeln.

Muster

Für Auftragsverarbeitungsverträge gemäß der DSGVO kursieren bereits einige Musterverträge. Diese sollten Sie keinesfalls unreflektiert übernehmen. In der Regel fehlt es bei solchen Vorlagen an ausreichenden Erläuterungen. Auch werden häufig sinnvolle Kostenregelungen vergessen oder Gestaltungsspielräume zu Gunsten der Auftragsverarbeiter nicht ausgeschöpft. Gleiches gilt für Verträge, die Ihnen möglicherweise von Kunden vorgelegt werden. Aufgrund der schärferen Regelungen der DSGVO dürfen Sie solche Verträge nicht als lästiges Beiwerk oder bloßen Papierkram ansehen.

IHRE TO-DOS:

- *DSGVO-konforme Auftragsverarbeitungsverträge mit Kunden abschließen und alte Auftragsdatenverarbeitungsverträge (nach § 11 BDSG-1990) überarbeiten.*
- *Mustervertrag entwickeln, der der DSGVO und Ihren individuellen Anforderungen gerecht wird.*
- *Auftragsverarbeitungsverträge, die von Kunden vorgelegt werden nicht sorglos unterschreiben, sondern prüfen.*

TO-DO 2:

Verfahrensverzeichnis führen

Verzeichnis der Verarbeitungstätigkeiten erstellen.

Datensicherheitsmaßnahmen dokumentieren.

Organisatorisch sicherstellen, dass das Verzeichnis fortgeführt wird und aktuell bleibt.

VERFAHRENSVERZEICHNIS FÜHREN

Ab dem 25. Mai 2018 müssen Sie auch als Auftragsverarbeiter ein sogenanntes „Verzeichnis der Verarbeitungstätigkeiten“ führen, Art. 30 Abs. 2 DSGVO. In diesem ist jedes Produkt bzw. jede Leistung, die Sie als Auftragsverarbeiter anbieten, aufzulisten (z.B. „Web-Hosting“, „Bereitstellung einer Online-Software zum Flottenmanagement“, „Betrieb und Wartung eines Online-Shops“). Ergänzend ist jeweils anzugeben, ob Sie hierbei einen Unterauftragnehmer außerhalb des Europäischen Wirtschaftsraums (EWR) einsetzen (z.B. Amazon oder Google Cloud Server), und ggf. in welchem Land sich dieser befindet. Für jedes Produkt bzw. jede Leistung müssen Sie im Verzeichnis der Verarbeitungstätigkeiten außerdem eine allgemeine Beschreibung der Maßnahmen beifügen, die Sie zur Datensicherheit getroffen haben. Dies betrifft Maßnahmen zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität ihrer Kundendaten (z.B. Zugangskontrolle in Büroräumen und Rechenzentren, Passwortrichtlinien, Backup- und Ausfallschutz).

Schließlich muss das Verzeichnis für jedes Produkt bzw. jede Leistung eine Liste aller zugehöriger Kunden beinhalten. Neben Namen und Kontaktdaten der Kunden sind dort auch die Kontaktdaten des Datenschutzbeauftragten des Kunden aufzunehmen. Bei Kunden außerhalb der EU müssen Sie zudem die Kontaktdaten von dessen Vertreter in der EU dokumentieren, wenn der Kunde den Bestimmungen der DSGVO unterliegt (z.B. Kunden in den USA, die ihre Leistungen EU-Bürgern anbieten und dabei deren Daten verarbeiten).

Das Führen des Verzeichnisses der Verarbeitungstätigkeiten bringt einen gewissen Verwaltungsaufwand mit sich, sollte aber nicht vernachlässigt werden. Datenschutz-Aufsichtsbehörden ist das Verzeichnis auf Anfrage vorzulegen, Art. 30 Abs. 4 DSGVO. Verstöße gegen die Dokumentationspflicht können mit einem Bußgeld geahndet werden, Art. 83 Abs. 4 a) DSGVGO.

Auch der Gesetzgeber hat offenbar den hinter dem Verzeichnis steckenden Verwaltungsaufwand erkannt und eine Ausnahme von der Dokumentationspflicht für Unternehmen mit weniger als 250 Mitarbeitern eingeführt, Art. 30 Abs. 5 DSGVO. Die Ausnahme greift aber nur ein, wenn gleichzeitig (Achtung die deutsche Übersetzung der DSGVO ist hier fehlerhaft) drei zusätzliche Voraussetzungen erfüllt sind. Unter anderem muss die Datenverarbeitung lediglich „gelegentlich“ erfolgen, damit die Dokumentationspflicht entfällt. Wenn Sie als Auftragsverarbeiter Ihren Kunden Leistungen anbieten, verarbeiten Sie aber deren Daten in der Regel nicht nur gelegentlich. Im Ergebnis kommen Sie damit kaum herum, ein entsprechendes Verzeichnis zu führen.

IHRE TO-DOS:

- *Verzeichnis der Verarbeitungstätigkeiten erstellen, in dem Ihre Produkte und Leistungen als Auftragsverarbeiter sowie Ihre Kunden aufgeführt sind.*
- *Datensicherheitsmaßnahmen dokumentieren und Beschreibung in das Verzeichnis aufnehmen.*
- *Organisatorisch sicherstellen, dass das Verzeichnis fortgeführt wird und aktuell bleibt.*

TO-DO 3:

Weisungen einfordern und managen

Umgang mit Weisungen (Form, Grenzen, Zuständigkeiten) im Vertrag mit Kunden regeln.

Mitarbeiter über die Bedeutung von Weisungen informieren und deren Einhaltung sicherstellen.

Erforderlichenfalls Weisungen vom Kunden aktiv einfordern.

WEISUNGEN EINFORDERN UND MANAGEN

Als Auftragsverarbeiter müssen Sie beim Umgang mit personenbezogenen Daten Ihrer Kunden deren „Weisungen“ befolgen. Das Gesetz geht davon aus, dass der Kunde seinem Auftragsverarbeiter Vorgaben zum Datenumgang in Form von Weisungen macht. Dies müssen Sie vertraglich so auch vereinbaren, Art. 28 Abs. 3 Satz 2 Buchstabe a DGVO.

Beispiel „Weisung Speicherdauer“: Sie entwickeln für einen Kunden eine Gutschein-App und betreiben das zugehörige Backend (Server). Der Kunde teilt Ihnen später mit, dass die Daten der Gutschein-Inhaber innerhalb von sechs Monaten nach Einlösen eines Gutscheins gelöscht werden sollen.

Beispiel „Weisung Datenumfang“: Sie bieten eine Online-Software für die Optimierung von Lieferketten an und übernehmen das initiale Customizing. Der Kunde bittet Sie, beim Einspielen der Kundendaten nur die Postleitzahl zu importieren, nicht jedoch die vollständige Kundenanschrift.

Häufig sind solche „Weisungen“ im Rahmen von Leistungsbeschreibungen, Aufträgen oder Produktspezifikationen bereits enthalten. Grundsätzlich hat der Kunde aber kraft Gesetzes das Recht Ihnen auch später jederzeit Weisungen zum Datenumgang zu erteilen.

Diese Weisungsabhängigkeit ist keine Neuerung der DSGVO gegenüber dem BDSG-1990. Unter der DSGVO ist es aber für Sie als Auftragsverarbeiter besonders wichtig, Weisungen erforderlichenfalls einzufordern, erteilte Weisungen zu befolgen und dies zu dokumentieren:

Verarbeiten Sie personenbezogene Daten Ihrer Kunden nämlich nicht nach dessen Weisungen, sondern legen wesentliche Fragen des „Wie“ der Datenverarbeitung selbst fest, werden Sie vom bloßen Auftragsverarbeiter zum „Verantwortlichen“ im Sinne der DSGVO, Art. 28 Abs. 10 DSGVO. Das heißt: Wenn Sie eigenmächtig Kernfragen des Datenumgangs festlegen oder gar Weisungen des Kunden missachten, sind Sie für die Einhaltung der Bestimmungen der DSGVO voll verantwortlich und haften z.B. gegenüber Betroffenen in erweitertem Umfang, vgl. Art. 82 Abs. 2 Satz 2 DSGVO.

Achten Sie also darauf, dass mit dem Kunden zentrale Fragen des Datenumgangs vereinbart oder vom Kunden festgelegt werden und dokumentieren Sie dies. Zentrale Fragen des Datenumgangs sind insbesondere der Umfang der erhobenen Daten, die Nutzungszwecke, die Weitergabe an Dritte und die Speicherdauer.

Beispiel „Vom Auftragsverarbeiter zum Verantwortlichen“: Sie bieten eine web-basierte Zeiterfassungssoftware für Unternehmen an. In der zugehörigen App wird bei der Eingabe von Zeiteinträgen auch der Gerätestandort erfasst. Der Standort wird zunächst nicht weiter genutzt, sondern soll für zukünftige Funktionen vorgehalten werden. Der Administrator des Kunden kann den Standort bei einem Daten-Export sehen. Die Erfassung der Standortdaten ist in Ihrer Leistungsbeschreibung aber nicht dokumentiert und kann vom Kunden auch nicht deaktiviert werden. Da eine Beauftragung bzw. Weisung des Kunden zur Erhebung der Standortdaten fehlt, sind Sie rechtlich voll verantwortlich für die Erfassung dieser Daten. Als Datensammlung „auf Vorrat“ ist diese rechtswidrig. Sie haften unmittelbar gegenüber den Mitarbeitern ihrer Kunden wegen unzulässigen Datensammelns.

Stellen Sie zudem durch vertragliche Vereinbarungen mit dem Kunden und durch entsprechende innerbetriebliche Organisation sicher, dass Weisungen des Kunden dokumentiert und umgesetzt werden.

Beispiel: „Die verlorene Weisung“: Sie sind Inhaber eine Webagentur. Ein langjähriger Großkunde möchte Sie mit der Schaltung einer Werbekampagne auf Facebook beauftragen. Ihr Social Media Experte empfiehlt zur besseren Ausrichtung der Kampagne „Facebook Custom Audiences“ zu nutzen und hierfür die Liste der Newsletter-Abonnenten des Kunden bei Facebook hochzuladen (Facebook nutzt diese Daten, um die Anzeigen bei der passenden Zielgruppe zu platzieren). Kurz nach Beauftragung teilt der Datenschutzbeauftragte des Kunden per Online-

Kontaktformular über Ihre Webseite mit, dass er ein Hochladen der Kundenliste für unzulässig hält und dies zu unterbleiben hat. Die E-Mail gelangt nicht rechtzeitig zu Ihrem zuständigen Mitarbeiter, der die Kundenliste bereits bei Facebook eingestellt hat.

Um sicherzustellen, dass Weisungen nicht verloren gehen, sollte festgelegt sein, wer auf Kundenseite Weisungen erteilen darf, wer der Empfänger in Ihrem Unternehmen ist und in welcher Form Weisungen dokumentiert werden müssen. Zudem müssen Sie Ihre Mitarbeiter über die Bedeutung von Kundenweisungen informieren und deren Beachtung sicherzustellen.

Wenn es um Kernfragen des Datenumgangs geht sollten Sie zudem im Einzelfall Weisungen aktiv einfordern. Dies gilt etwa in Bezug auf eine Datenverarbeitung außerhalb der EU, Art. 28 Abs. 3a) DSGVO.

Beispiel: „Die einzufordernde Weisung“: Sie erbringen remote Wartungsleistungen für eine beim Kunden installierte CRM-Software. Der Kunde bittet Sie kurzfristig ein „Cloud-Backup“ aller Kundendaten zu erstellen. Fehlen dabei Vorgaben, etwa zum Speicherort (EU, USA), empfiehlt es sich, auf den Kunden zuzugehen und um eine entsprechende Konkretisierung des Auftrags zu bitten bzw. um ausdrückliche Bestätigung, ob die von Ihnen vorgeschlagene Lösung in Ordnung ist.

Zudem verlangt die DSGVO, wie auch schon das BDSG-1990, dass Sie Ihre Kunden informieren, wenn Sie eine Weisung für datenschutzwidrig halten. Eine rechtliche Prüfpflicht entsteht für Sie dadurch aber nicht.

IHRE TO-DOS:

- *Umgang mit Weisungen (Form, Grenzen, Zuständigkeiten) im Vertrag mit ihren Kunden regeln.*
- *Mitarbeiter über die Bedeutung von Weisungen informieren und deren Einhaltung sicherstellen.*
- *Erforderlichenfalls Weisungen vom Kunden aktiv einfordern.*

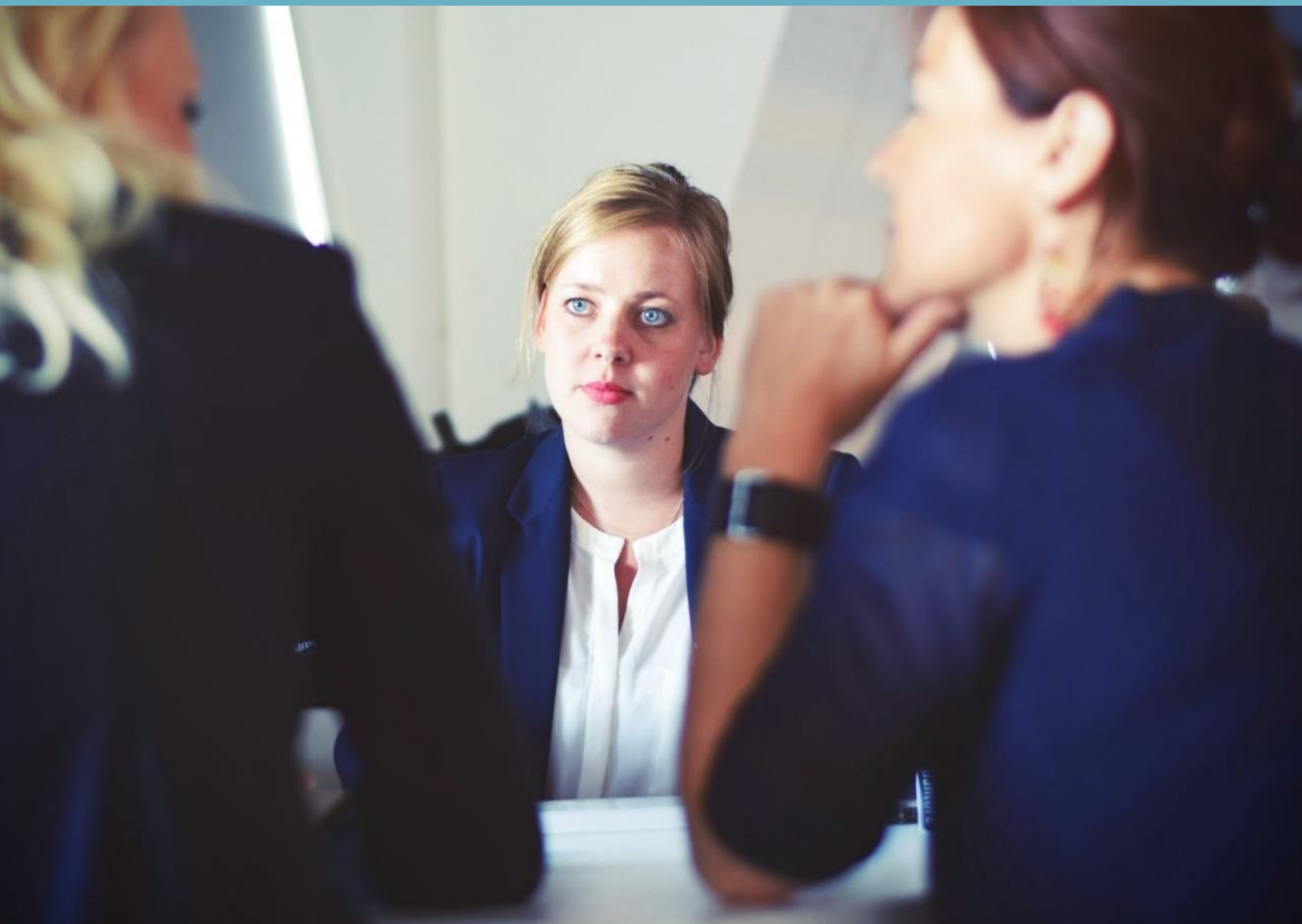
TO-DO 4:

Datenschutzbeauftragten benennen

Prüfen, ob ein Datenschutzbeauftragter bestellt werden muss oder soll.

Internen oder externen Datenschutzbeauftragten bestellen.

Bei der Bestellung Aufgaben des Datenschutzbeauftragten konkret regeln.



DATENSCHUTZBEAUFTRAGTEN BENENNEN

Wenn sich in Ihrem Unternehmen in der Regel zehn oder mehr Personen mit der Verarbeitung von personenbezogenen Daten beschäftigen, müssen Sie einen Datenschutzbeauftragten benennen, § 38 Abs. 1 BDSG-2017, Art. 37 Abs. 1 DSGVO. Mitzuzählen sind z.B. alle Entwickler, die Zugriff auf Kundendaten haben sowie Beschäftige im Support, die auf Kundendaten zugreifen können. Auch Mitarbeiter, die sich um ihr Personal kümmern (Personalabteilung) zählen dazu.

In Sonderfällen besteht eine Benennpflicht auch, wenn Sie die Personenzahl von zehn nicht erreichen. Dies ist unter anderem dann der Fall, wenn Ihre Geschäftstätigkeit im Kern darin besteht, in großem Umfang Gesundheitsdaten zu verarbeiten, wenn Sie besonders risikoreiche Datenverarbeitungen durchführen (vgl. § 28 Abs. 1 BDSG-2018, Art. 35 DSGVO) oder wenn Sie ein Markt- oder Meinungsforschungsinstitut sind.

Müssen Sie keinen Datenschutzbeauftragten benennen, können Sie dies dennoch freiwillig tun. Das kann durchaus sinnvoll sein, um eine definierte Rolle mit festgelegten Aufgaben zu etablieren, die sich des Themas im Unternehmen annimmt. Außerdem wirkt die Benennung eines Datenschutzbeauftragten gerade bei kleinen Unternehmen bei Kunden vertrauensbildend.

Der Datenschutzbeauftragte berät ihr Unternehmen und ihre Mitarbeiter zu den Datenschutz-Pflichten, nimmt Schulungen vor und überwacht die Einhaltung der Datenschutzbestimmungen, Art. 39 Abs. 1 DGVO. Vor allem die Kontrollpflichten des Datenschutzbeauftragten gehen nach der DGSVO über diejenigen des BDSG-1990 hinaus. Sie müssen den Datenschutzbeauftragten hierfür in alle datenschutzrelevanten Sachverhalte einbinden, Art. 38 Abs. 1 DGVO und ihm ausreichend Ressourcen (Zeit, Geld, Informationen) zur Verfügung stellen, Art. 38 Abs. 3 Satz 1 DSGVO. Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen (z.B. auf ihrer Webseite) und der für Sie zuständigen Datenschutzbehörde mitzuteilen, Art. 37 Abs. 7 DSGVO. Diese Transparenz-Anforderungen sind gegenüber dem BDSG-1990 neu.

Zum Datenschutzbeauftragten können Sie einen eigenen Mitarbeiter oder einen externen Dienstleister benennen. Die Person muss über die erforderliche Fachkunde verfügen und darf keinen Interessenskonflikt haben, also nicht seine eigene Arbeit kontrollieren. Geschäftsführer, führende Mitarbeiter der IT oder der Personalleiter können also nicht benannt werden. Wenn Sie einen eigenen Mitarbeiter benennen (interner Datenschutzbeauftragter), hat dies den Vorteil, dass dieser in Ihre Geschäftsprozesse gut integriert ist und „den Laden“ kennt. Allerdings müssen Sie Zeit und Geld in dessen Aus- und Fortbildung stecken. Außerdem genießt der Datenschutzbeauftragte – sofern eine Bestellpflicht vorliegt – einen Sonderkündigungsschutz, §§ 38 Abs. 2, 6 Abs. 4 BDSG-2018. Ein externer Datenschutzbeauftragter dagegen muss bezahlt werden und kennt ihr Unternehmen nicht so gut. Er kann dafür Datenschutzexpertise bündeln und effizient beraten, wenn er mehrere Unternehmen der gleichen Branche vertritt. Außerdem haben Sie bei einem externen Datenschutzbeauftragten das Haftungsrisiko ausgelagert: bei unzureichender Arbeit eines angestellten (internen) Datenschutzbeauftragten sind ihre Ansprüche in Haftungsfällen nach arbeitsrechtlichen Grundsätzen eingeschränkt, diese Haftungsbegrenzung gilt bei Externen nicht.

Immer wieder entsteht der falsche Eindruck, der Datenschutzbeauftragte sei für die Einhaltung der Datenschutzvorschriften verantwortlich. Das ist falsch. Verantwortlich ist die Unternehmensleitung. Der Datenschutzbeauftragte hat lediglich eine beratende und kontrollierende Rolle.

Dem Datenschutzbeauftragten obliegt es kraft Gesetz auch nicht, das Verzeichnis der Verarbeitungstätigkeiten zu führen oder Verträge zur Auftragsdatenverarbeitung zu entwerfen oder zu unterzeichnen. Auch muss der Datenschutzbeauftragte keine internen Anweisungen zum Datenschutz verfassen, kraft Gesetzes obliegt ihm lediglich die „Überwachung“

der Strategien und Richtlinien des Unternehmens, Art. 39 Abs. 1 b) DSGVO. Solche Einzelheiten müssen Sie mit dem Datenschutzbeauftragten also konkret vereinbaren. Vor diesem Hintergrund empfiehlt es sich auch, bestehende Alt-Vereinbarungen mit Datenschutzbeauftragten bzw. Alt-Bestellungen nach dem BDSG-1990 zu erneuern. Bei Verträgen mit Externen ist der Leistungsumfang konkret zu prüfen und zu verhandeln.

Egal ob Sie einen Datenschutzbeauftragten benannt haben oder nicht: Die DSGVO müssen Sie in jedem Fall beachten. Deshalb bietet es sich ggf. an, wenn kein Datenschutzbeauftragter benannt ist, einer Person im Unternehmen Aufgaben zur Einhaltung des Datenschutzes zu übertragen. Diese sollten Sie dann zur Klarheit nicht „Datenschutzbeauftragter" nennen, sondern z.B. „Datenschutzmanager".

IHRE TO-DOS:

- *Prüfen, ob ein Datenschutzbeauftragter bestellt werden muss oder soll.*
- *Internen oder externen Datenschutzbeauftragten bestellen.*
- *Bei der Bestellung Aufgaben des Datenschutzbeauftragten konkret regeln.*

TO-DO 5:

Einhaltung des Datenschutzes intern regeln und dokumentieren

Erstellen einer unternehmensinternen Datenschutzrichtlinie zur Sicherstellung der Einhaltung der DSGVO bei der Auftragsverarbeitung.

Mitarbeiter mit der Datenschutzrichtlinie vertraut machen und zur Einhaltung verpflichten.

EINHALTUNG DES DATENSCHUTZES INTERN REGELN UND DOKUMENTIEREN

Eine vergleichsweise knapp formulierte Vorschrift in der DGSVO hat es besonders in sich und hat bei vielen Unternehmen teils umfangreiche Datenschutzprojekte ausgelöst: Die sogenannte „Rechenschaftspflicht". Danach müssen Unternehmen den Datenschutz nicht nur einhalten, sondern dies auch *nachweisen* können, Art. 5 Abs. 2 DSGVO. Unternehmen geraten aufgrund der Rechenschaftspflicht in eine Art Beweispflicht. Der Druck datenschutzrelevante Prozesse im Unternehmen präzise zu regeln und zu dokumentieren steigt enorm. Art. 24 Abs. 1 DSGVO konkretisiert die Rechenschaftspflicht und verlangt, dass Unternehmen „angemessene technische und organisatorische Maßnahmen" treffen müssen, um die Einhaltung der DGSVO sicherzustellen und um hierfür auch den Nachweis erbringen zu können.

Im Hinblick auf mögliche Bußgelder von bis € 20.000.000 (Art 82 Abs. 5 DSGVO) erlangt die Rechenschaftspflicht zusätzliche Brisanz.

Für Sie kommt hinzu, dass sich Ihre Kunden eigentlich vorab, also bevor man Sie beauftragt, davon überzeugen müssen, dass Sie als Auftragsverarbeiter ausreichende Vorkehrungen zur Einhaltung der DSVGO getroffen haben, Art. 28 Abs. 1 DSGVO.

Unternehmensinterne Datenschutzrichtlinie

Als Fundament zur Erfüllung der DSGVO und Ihrer Rechenschaftspflicht sollten Sie eine unternehmensinterne Datenschutzrichtlinie aufsetzen, in der die wichtigsten Prozesse und Regeln in Bezug auf den Datenschutz festgelegt sind. Die Datenschutzrichtlinie bringen Sie ihren Mitarbeitern zur Kenntnis und verpflichten sie damit entsprechend zu handeln.

Bei Anfragen von Kunden können Sie Ihre Datenschutzrichtlinie vorlegen und so zeigen, dass Datenschutz bei Ihnen nicht nur in Marketingunterlagen steht, sondern real gelebt wird.

Eine unternehmensinterne Datenschutzrichtlinie bietet zudem den Vorteil, dass im Falle einer behördlichen Kontrolle oder eines Datenschutzverstoßes der Vorwurf eines Organisationsverschuldens besser abgewehrt werden kann. Sie können dann argumentieren, dass nur ein Fehler im Einzelfall vorliegt, was auch bei der Bemessung eines etwaigen Bußgelds zu Ihren Gunsten berücksichtigt wird. Auch in kleineren Unternehmen ohne internes „Richtlinienwesen" ist es daher sinnvoll eine interne Datenschutzrichtlinie zur Auftragsverarbeitung zu verfassen.

Inhalte für eine interne Datenschutzrichtlinie

In einer solchen unternehmensinternen Datenschutzrichtlinie bieten sich folgende Regelungen zu Verantwortlichkeiten und Prozessen an:

- **Auftragsverarbeitungsverträge mit Kunden**: Prozess zum Abschluss entsprechender Verträge, Verweis auf unternehmenseigene Musterverträge, Leitlinien beim Abschluss fremder Vertragsmuster („Do's and Don'ts").
- **Einschaltung von Unter-Auftragsverarbeitern**: Prozess zur Einschaltung von Unter-Auftragsverarbeitern, einschließlich vorheriger Prüfung und Mitteilung von Änderungen gegenüber Kunden, Audits und Kontrollen bei Unter-Auftragsverarbeitern.
- **Verzeichnis der Verarbeitungstätigkeiten**: Verantwortlichkeiten und Prozesse zur Führung des Verzeichnisses, ggf. Vorlage/Muster.
- **Management von Kunden-Weisungen**: Erläuterung der Bedeutung von Weisungen, Prozesse zur Behandlung und Dokumentation von Weisungen, Festlegung von Zuständigkeiten, Hinweispflicht gegenüber Kunden bei rechtlichen Bedenken, Pflicht zur Umsetzung von Weisungen.
- **Datenschutzbeauftragter**: Festlegung der Stellung und Aufgaben, Pflicht der

Mitarbeiter zur Einbindung des Datenschutzbeauftragten bei Datenschutzfragen.

- **Weitere Aspekte**: z.B. Prozess zur Verpflichtung von Mitarbeitern zur Vertraulichkeit (Art. 28 Abs. 3 b DSGVO), Umgang mit Anfragen von Betroffenen (Kunden ihrer Kunden) im Hinblick auf ihre Daten (vgl. Art. 12-22 DSGVO), Verweis auf Regelungen zur Datensicherheit, regelmäßige Prüfung bzw. Überarbeitung der Richtlinie.

IHRE TO-DOS:

- ⌦ *Erstellen einer unternehmensinternen Datenschutzrichtlinie zur Sicherstellung der Einhaltung der DSGVO bei der Auftragsverarbeitung.*
- ⌦ *Mitarbeiter mit der Datenschutzrichtlinie vertraut machen und zur Einhaltung verpflichten.*

TO-DO 6:

Datenschutz ins Produkt einbauen

Eigenes Produkt bzw. eigene Leistungen durch die Datenschutz-Brille des Kunden betrachten.

Soweit sinnvoll FAQs, Whitepaper oder Muster entwerfen, um den Kunden beim datenschutzkonformen Einsatz Ihres Produktes bzw. Ihrer Leistungen zu helfen.

Ggf. Produkt um Funktionen zum Datenschutz ergänzen.

DATENSCHUTZ INS PRODUKT EINBAUEN

Wenn Sie als Auftragsverarbeiter personenbezogene Daten ihrer Kunden verarbeiten, ist grundsätzlich der Kunde für die Zulässigkeit der Datenverarbeitung verantwortlich.

Beispiel „Verantwortlichkeit des Kunden“: Sie bieten Hosting-Dienstleistungen für Webseiten-Betreiber an. Es liegt in der Verantwortung des Kunden, mittels seiner Webseite Daten nur im zulässigen Umfang zu erfassen und zu speichern. Auch die Pflicht, die Webseitenbesucher über den Einsatz z.B. von Tracking-Tools (Google Analytics) zu informieren, oder registrierten Nutzern Auskunft zu ihren Daten zu erteilen, liegt vollständig im Verantwortungsbereich des Kunden.

Häufig ist es jedoch so, dass die Produkte bzw. Leistungen, die Sie als Auftragsverarbeiter anbieten, bereits einen gewissen Datenumgang aufgrund der mitgelieferten Funktionalität vorgeben oder implizieren. Dies gilt etwa bei Anbietern von Online-Software, die beim Anbieter betrieben und vom Nutzer per Browser verwendet wird („Software as a Service“).

Beispiel „Bewerbermanagement“: Sie bieten Unternehmen eine Online-Software zur Verwaltung von Stellenbewerbern an. Dabei werden standardmäßig bestimmte Daten von Bewerbern erfasst und vorgehalten, Auswertungen zum Vergleich verschiedener Bewerber angeboten, ein Tracking von Webseitenbesuchern durchgeführt und es sind definierte Rollen (z.B. „Recruiter“) mit festen Berechtigungen vorgesehen.

Helfen Sie Ihren (potentiellen) Kunden dabei, die Anforderungen der DSGVO bei der Inanspruchnahme ihrer Leistungen sicherzustellen. Gerade für größere und renommierte Kunden ist die Datenschutzkonformität eine wichtige Auswahlentscheidung. Das „Wie“ und teilweise „Ob“ vieler Projekte im Unternehmen wird heute - und in Zukunft noch mehr - vom Datenschutz beeinflusst. Wer es seinen Kunden beim Datenschutz leicht macht, der verkauft auch besser. Das gilt unter der DSGVO mehr denn je: Die DSGVO verpflichtet nämlich Ihre Kunden bereits im Zeitpunkt der Konzeption von Vorhaben, sicherzustellen, dass die Vorschriften der DSGVO eingehalten werden können. Diese Pflicht wird in der DSGVO als „Datenschutz durch Technikgestaltung“ (Privacy by Design) bezeichnet, Art. 25 Abs. 1 DSGVO.

Stellen Sie Kunden FAQs oder Whitepaper zum Datenschutz bereit, und erläutern Sie dort die wichtigsten Datenschutz-Fragen zu Ihrem Produkt. Entwerfen Sie Muster, die Ihre Kunden verwenden können und bauen Sie in Ihr Produkt Funktionen ein, die dem Kunden die Einhaltung der DSGVO erleichtern.

Welche Maßnahmen dabei sinnvoll sind, muss im Rahmen einer individuellen Betrachtung Ihrer Leistungen bzw. Ihres Produktes erfolgen. Mit Blick auf die mit der DSGVO einhergehenden Neuerungen im Datenschutz sind folgende drei Aspekte hervorzuheben:

Transparenzpflichten

Die DSGVO verlangt von Ihren Kunden, die Personen, deren Daten Ihr Kunde verarbeitet (Betroffene), umfassend über den Datenumgang zu informieren (z.B. Dauer der Speicherung, Weitergabe an Dritte, Übermittlung in Länder außerhalb der EU). Diese Transparenzpflichten wurden mit der DSGVO gegenüber dem BDSG-1990 deutlich erhöht (siehe etwa Art. 13, 14 und 21 DSGVO). Gerade bei „Software as a Service“ Produkten wissen Sie als Anbieter oft besser als der Kunde, was mit den Daten passiert. Es bietet sich dann an, dem Kunden Muster für Datenschutzhinweise bereitzustellen oder konkrete Erläuterungen, anhand derer der Kunde solche Datenschutzhinweise selbst erstellen kann.

Betroffenenrechte

Die DSGVO stärkt und erweitert teilweise die Rechte der Betroffenen. So können Betroffene von Ihren Kunden in bestimmten Fällen verlangen, dass der Kunde alle zur betroffenen Person gespeicherten Daten in einem „strukturiertem, gängigen und maschinenlesbaren Format“ bereitstellt (sogenanntes „Recht auf Datenübertragbarkeit“, Art. 20 DSGVO). Sie können dem Kunden hierzu entsprechende Funktionalitäten oder Leistungen bereitstel-

len, die einen entsprechenden Datenexport auf Knopfdruck ermöglichen (z.B. als XML oder CSV-Datei).

Datenschutzfreundliche Voreinstellungen

Können Standardeinstellungen zum Umgang mit personenbezogenen Daten festgelegt werden, so sind diese möglichst „datenschutzfreundlich" vorzunehmen. Dieser Grundsatz des „Privacy by Default" wurde mit der DSGVO explizit geregelt, Art. 25 Abs. 2 DSGVO. Das heißt, dass mit Blick auf den Nutzungszweck Ihr Produkt nicht mehr Daten als nötig, nicht länger als nötig und nicht umfassender als nötig verarbeiten darf, und der Zugriff durch Dritte standardmäßig soweit wie möglich eingeschränkt sein muss.

Beispiel „Enterprise Social Network": Sie bieten ein Standardprodukt an, mit dem Kunden ein Unternehmensinternes soziales Netzwerk betreiben können. Die Voreinstellungen sollten möglichst restriktiv gesetzt werden, z.B. in Bezug auf die Frage welche Personen ein Profilbild sehen können oder ob Standortdaten bei Statusmeldungen angezeigt werden.

Neben diesen Punkten sind für einen datenschutzkonformen Einsatz Ihres Produkts bzw. Ihrer Leistungen häufig ein abgestuftes Rollen- und Berechtigungskonzept sowie definierbare Löschregeln für personenbezogene Daten wichtig.

IHRE TO-DOS:

- *Eigenes Produkt bzw. eigene Leistungen durch die Datenschutz-Brille des Kunden betrachten.*
- *Soweit sinnvoll FAQs, Whitepaper oder Muster entwerfen, um den Kunden beim datenschutzkonformen Einsatz Ihres Produktes bzw. Ihrer Leistungen zu helfen.*
- *Ggf. Produkt um Funktionen zum Datenschutz ergänzen.*

IHRE NÄCHSTEN SCHRITTE

Schieben Sie die Anforderungen der DSGVO nicht beiseite. Das Thema ist wichtig aufgrund des Haftungs- und Bußgeldrisikos und zur Sicherung der Kundenbeziehung.

Die Umsetzung der DSGVO bringt einen gewissen Aufwand mit sich, doch Sie müssen nicht bei Null anfangen: Nutzen Sie das von mir entwickelte „DSGVO-Kit“. Mit diesem können Sie einen Großteil der beschriebenen Anforderungen professionell und effizient umsetzen. Das Paket berücksichtigt eine lange Erfahrung in der Rechtsberatung vieler Auftragsverarbeiter. Es beinhaltet:

- *Schritt-für-Schritt Anleitung zur Umsetzung der DSGVO für Auftragsverarbeiter*
- *Muster für eine unternehmensinterne Datenschutzrichtlinie (Arbeitsanweisung)*
- *optimierter Mustervertrag zur Auftragsverarbeitung mit Kunden*
- *Checkliste zur Prüfung von fremden Verträgen zur Auftragsverarbeitung*
- *Vorlage für ein „Verzeichnis der Verarbeitungstätigkeiten“*

Alle Vorlagen sind bearbeitbar (Word-Dateien) und gut kommentiert. Das DSGVO-Kit richtet sich an Inhaber, Geschäftsführer, Projektverantwortliche, Inhouse-Juristen, Rechtsanwälte sowie interne und externe Datenschutzbeauftragte. Es sind weder Vorkenntnisse zur DSGVO noch eine juristische Ausbildung erforderlich.

Weitere Informationen zum DSGVO-Kit sowie eine Bestellmöglichkeit finden Sie auf der Webseite des Verlags unter:

www.complyvacy.com/dsgvo-kit

[1] *Bei dem DSGVO-Kit handelt es sich um ein Verlagsprodukt und nicht um individuelle Rechtsberatung.*

Rechtsanwaltskanzlei
Dr. Thomas Helbing
Fachanwalt für IT-Recht

Kopernikusstr. 9
81679 München

+49 (0) 89 - 45 70 84 05
helbing@thomashelbing.com
www.thomashelbing.com