Your World First

C/M/S/
Law.Tax

In 7 Schritten zur DSGVO

Wie Sie sich auf die neue Datenschutz-Grundverordnung der EU vorbereiten. Welche empfindlichen Strafen künftig drohen; und warum nun auch KMU für Compliance sorgen müssen.

September 2017

in Kooperation mit

INDUSTRIE MAGAZIN

Die neue DSGVO trifft alle.

Außer Ingo – er sammelt keine Daten.

INHALT

Die Zeit drängt

Im Mai 2018 tritt die neue Datenschutz-Grundverordnung der EU in Kraft. Bei Verstößen drohen Strafen bis 20 Millionen Euro oder vier Prozent des Umsatzes. Unternehmen müssen daher jetzt Vorbereitungen treffen – egal ob Konzern oder KMU.

Die Digitalisierung wirbelt eine Reihe von Geschäftsmodellen durcheinander: Produktionsbetriebe können per Webshop direkt an den Endkunden liefern, Ersatzteile werden im Webshop des Lieferanten bestellt, die Lohnbuchhaltung an einen externen Dienstleister ausgelagert. Das neue Öl, das dies alles ins Laufen bringt, sind bekanntlich Daten. Für die EU ein Grund, den Rahmen für die Sammlung und Übermittlung von Daten genau abzustecken.

So tritt mit 25. Mai 2018 die neue Datenschutz-Grundverordnung (DSGVO) in Kraft, die die Betroffenenrechte stärken soll. Ziel ist es aber auch, einheitliche Standards im Datenschutz innerhalb der EU zu gewährleisten sowie den grenzüberschreitenden Datenaustausch innerhalb Europas zu vereinfachen.

Dennoch wird für die Unternehmen zunächst einmal alles aufwändiger.

Mehr mit Datenschutz auseinandersetzen

Gerade aus österreichischer Sicht macht die DSGVO einiges anders als bisher gewohnt: Zum Beispiel wird es künftig keine Meldung bei der Datenschutzbehörde mehr geben. Stattdessen müssen sich die Verantwortlichen selbst stärker um die Sicherheit und den Datenschutz bei ihrer Datenverarbeitung kümmern. An die Stelle der Eintragung ins Datenverarbeitungsregister bei der Behörde tritt nämlich die Erstellung eines eigenen Verarbeitungsverzeichnisses.

Geschäftsführer, Marketing- und HR-Verantwortliche, aber auch andere Personen im Unternehmen werden sich also viel

stärker mit dem Thema auseinandersetzen müssen als bisher. Am besten ist es daher, schon jetzt die nötigen Schritte zur Vorbereitung auf die DSGVO einzuleiten. Denn die DSGVO verstärkt die bisherigen Pflichten: Ab Inkrafttreten besteht beispielsweise eine Auskunftspflicht darüber, welche personenbezogenen Daten zu welchem Zweck erhoben werden sowie auch darüber, wie die Löschung von Daten gehandhabt wird. Das betrifft auch das Verhältnis zu Auftragsverarbeitern, also zu jenen Unternehmen, die die Daten im Auftrag verarbeiten.

Brisanz gewinnt das Thema Datenschutz auch deshalb, weil die EU die Strafen massiv verschärft hat: Waren in der Vergangenheit bei Datenschutzverletzungen in Österreich max.10.000 bis 25.000 Euro zu bezahlen, sieht die DSGVO bei Verstößen Strafzahlungen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Umsatzes vor; eine Summe also, die weh tut und daher zeigt, wie notwendig eine rechtzeitige Befassung mit der DSGVO ist.

Nahezu alle sind betroffen

Von der DSGVO betroffen sind – wenn auch nicht in gleichem Ausmaß – übrigens so gut wie alle Unternehmen. Selbst viele KMU, die sich bis dato wenig mit Datenschutz beschäftigt haben, zeichnen Kunden- oder Mitarbeiterdaten auf. Auch sie müssen daher künftig ein Verarbeitungsverzeichnis vorlegen können. Wie viel Arbeit und IT-Ressourcen Unternehmen dafür investieren müssen, hängt freilich vom Risiko ab, das für Betroffenenrechte im Betrieb besteht. Wer zum Beispiel sensible Daten wie Gesundheitsdaten verarbeitet, hat ungleich mehr Aufwand als andere.

Zeit für Adaptierungen nutzen

Was genau zu tun ist, um die Umstellung ohne größere Probleme zu meistern, ist in den folgenden sieben Schritten skizziert. Während einige Unternehmen jeder Schritt betreffen wird, haben andere hingegen nur einzelne Schritte zu setzen. Für alle jedoch gilt: Bis Inkrafttreten der DSGVO ist nicht mehr viel Zeit. Man sollte sie für die nötigen Adaptierungen im Unternehmen nutzen.
Mehr Info unter:
https://cms.law/de/AUT/DSGVO

1. Dokumentieren Sie Ihre Datenflüsse

In einem ersten Schritt heißt es, Inventur zu machen: Prüfen Sie, welche Daten im Unternehmen überhaupt verarbeitet werden. Nur so können Sie Fehler beim Erstellen eines Verzeichnisses der Datenflüsse vermeiden.

Die Übergangszeit für die Erfüllung der (vollständigen) Anforderungen der DSGVO endet am 25. Mai 2018. Ab diesem Zeitpunkt müssen die Verarbeitungen beim Verantwortlichen den Anforderungen der DSGVO genügen. Die erste Herausforderung zu einer datenschutzrechtlich konformen Compliance-Kette stellt die Erstellung des Verarbeitungsverzeichnisses dar.

Dieses Verarbeitungsverzeichnis soll der Datenschutzbehörde die Möglichkeit bieten, die betreffenden Verarbeitungsvorgänge zu kontrollieren. Dies hat wiederum zur Konsequenz, dass in diesem Verzeichnis alle Datenverarbeitungen zu führen sind, welche von Ihrem Unternehmen getätigt werden. Folglich ist es Ihr Ziel, in einem ersten Schritt alle Datenverarbeitungsprozesse zu identifizieren und diese entsprechend schriftlich oder elektronisch zu dokumentieren und sie dann kompakt in einem Verzeichnis darzustellen.

Die Anforderungen an Ihr Unternehmen auf einen Blick

Dynamisches Verzeichnis: Das Verarbeitungsverzeichnis ist „dynamisch". Das bedeutet, dass jede identifizierte bzw. definierte Tätigkeit in regelmäßigen Abständen darauf zu überprüfen ist, ob die Prozesse auch genauso ablaufen, wie ursprünglich festgestellt und dokumentiert. Wenn sich also Verarbeitungstätigkeiten z. B. aufgrund geänderter Anforderungen ändern, sind diese Änderungen auch im Verzeichnis darzustellen. Es ist daher empfehlenswert, auch nach Erstellen des Verzeichnisses ca. einmal jährlich die zuständigen Auskunftspersonen der betroffenen Abteilungen zu konsultieren.

Historie: Ihr Unternehmen trifft die

Pflicht als Verantwortlicher, (jederzeit) nachweisen zu können, dass die Datenverarbeitung (zu jeder Zeit) rechtskonform erfolgt. Diese Anforderung hat mithin zur Konsequenz, dass dieses Verzeichnis eine Historie enthalten muss, die entsprechend gepflegt wird, um die Einhaltung der Vorgaben auch für einen zurückliegenden Zeitraum nachweisen zu können.

Ansprechpartner: Diesbezüglich sieht die DSGVO zwingend nur den oder die Verantwortlichen sowie dessen Vertreter und – sofern vorhanden – Datenschutzbeauftragten vor. Es erleichtert jedoch die Arbeit der Datenschutzbehörde und vermindert die Nachfragen bei einer ggfs. stattfindenden Überprüfung, wenn zusätzlich zu den explizit geforderten Angaben zumindest die für die entsprechenden Verarbeitungstätigkeiten relevanten Personen (z. B. HR-Leiter, IT-Leiter, etc.) im Verzeichnis mit angeführt werden.

„Datamapping" – Ermittlung der Daten

Um einen Überblick über die Datenverarbeitung zu bekommen und um ein

Wichtige Fragen:

Wer?

Prüfen Sie, von welchen natürlichen Personen Sie Daten erhalten.

Warum?

Klären Sie, zu welchem Zweck Sie personenbezogene Daten brauchen.

Welche?

Hinterfragen Sie, welche Daten Sie genau (mit-)erheben und welche Sie nutzen.

Wie?

Sie müssen sich auch damit auseinandersetzen, wie Sie an die Daten kommen.

Wie lange?

Schließlich müssen Sie auch regeln, wie lange Sie die Daten aufbewahren. Um einen Überblick über die Datenverarbeitung zu bekommen und um ein vollständiges und aktuelles Verarbeitungsverzeichnis zu erstellen, müssen Sie **folgende Fragen stellen:**

vollständiges und aktuelles Verarbeitungsverzeichnis zu erstellen, sollen Sie folgende Fragen stellen:

Von wem brauchen Sie personenbezogene Daten? Abhängig von dem Unternehmen und der Abteilung, in der Sie arbeiten, könnten Sie z. B. in Kontakt mit den Daten von Bewerbern, Mitarbeitern, Lieferanten, Spediteuren, Verbrauchern, potenziellen Interessenten, eigenen Kunden, Kontaktpersonen beim Kunden, an der Geschäftsabwicklung mitwirkenden Dritten, Organen (und deren Mitglieder) und sonstigen Funktionsträgern von juristischen Personen, etc. kommen.

Zu welchem Zweck brauchen Sie die Daten? Hier geht es um die Frage, warum Sie die personenbezogenen Daten brauchen. Sind Sie z. B. in der Logistik oder im Rechnungswesen tätig und brauchen die Daten im Rahmen der Geschäftsbeziehung mit Kunden? Oder sind Sie in der Personalverwaltungsabteilung tätig und brauchen die Daten für die Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten?
Oder sind Sie vielleicht für das Marketing Ihres Unternehmens zuständig und verwenden die eigenen oder zugekaufte Kunden- und Interessentendaten für eine Geschäftsanbahnung?

Welche Daten nutzen Sie? Abhängig davon, von welchen natürlichen Personen Sie Daten erheben und zu welchem Zweck Sie diese nutzen, können die verschiedensten Daten mitumfasst sein.

Q: **Ich habe auf einer Veranstaltung Visitenkarten erhalten. Darf ich die in meine Kundendatei aufnehmen?**

A: „Grundsätzlich ja. Neben einer wirksamen Einwilligung (und anderen rechtlichen Voraussetzungen) ist der Zweck der Datenverarbeitung genau zu definieren." Dr. Johannes Juranek, Partner CMS

Wenn Sie z. B. die Daten für die Verwaltung von Geschäftsbeziehungen mit Kunden oder zum Management der Kundenzufriedenheit erheben, werden Sie aller Wahrscheinlichkeit nach Daten wie Kundennamen, Namen der Ansprechperson beim Kunden, interne Kundennummer, Adressdaten (z. B. Ort der Niederlassung), Kontaktdaten (E-Mail-Adresse, Faxnummer, Telefonnummer), verarbeiten. Sind Sie hingegen in der HR-Abteilung tätig, werden Sie vorwiegend mit Mitarbeiter- oder Bewerberdaten in Berührung kommen, die z. B. Angaben zur Person (Name, Anschrift, Geburtsdatum) oder das Beschäftigungsverhältnis (Vollzeit/Teilzeit, Gehalt, Dauer der Betriebszugehörigkeit, Vorgesetzter, Tätigkeiten im Unternehmen) betreffen könnten.

Wie kommen Sie zu den Daten?
Schließlich müssen Sie sich mit der Frage auseinandersetzen, wie Sie die Daten von den Betroffenen erhalten. Betreibt Ihr Unternehmen z. B. einen Onlineshop, auf dem der Kunde online Waren kaufen kann? Dann werden Sie die Kundendaten aller Wahrscheinlichkeit nach für die Warenzustellung benötigen, weil Sie sonst die vertragliche Beziehung mit dem Kunden nicht erfüllen können. Oder sind Sie in der HR-Abteilung tätig und brauchen die Daten von neu eingestiegenen Mitarbeitern, um der Sozialversicherung das Beschäftigungsverhältnis anzuzeigen? In einem solchen Fall sind die Daten für Sie notwendig, um den Ihrem Unternehmen rechtlich auferlegten Pflichten nachzukommen.

2. Holen Sie sich Einwilligungen

Der Versand von Werbemails oder Newslettern kann zum Stolperstein werden. Denn Zusendungen zu Werbezwecken sind außerhalb aufrechter Geschäftsbeziehungen unzulässig, außer Sie haben vorher eine wirksame Einwilligung des Betroffenen eingeholt.

Grundsätzlich gilt, dass jede Zusendung zu Werbezwecken unzulässig ist, wenn sie ohne vorherige Einwilligung des Betroffenen oder an mehr als 50 Adressaten versandt wird. Das Einholen der konkreten Einwilligung fällt dann weg, wenn:

- **Die Kontaktadresse** dem Versender innerhalb eines Geschäftsprozesses mitgeteilt wurde und
- **der Versender** diese Kontaktadresse nur zur Bewerbung weiterer eigener Angebote nutzt und
- **der Betroffene** den Empfang der Werbemails im gesamten Kommunikationsprozess jederzeit und kostenfrei ablehnen kann.

Geben Sie sich zu erkennen

Vergessen Sie nicht, eine offizielle Firmen-E-Mail-Adresse zu nutzen und platzieren Sie sichtbar im Werbemail einen „Unsubscribe" Link, der es dem Betroffenen ermöglicht, jederzeit weiteren Zusendungen zu widersprechen. Denken Sie auch daran, dass jeder Newsletter bzw. Werbemail als solche gekennzeichnet sein muss, z. B. durch einen eindeutigen Hinweis in der Betreffzeile. Bedenken Sie auch, dass der Absender zu jeder Zeit klar erkennbar sein muss; das heißt, dass er auf seiner Website über ein Impressum verfügen und in der E-Mail-Signatur mit seinen Kontaktinformationen aufscheinen muss.

Das „Ja, ich will"-Dilemma

Nun stellen Sie sich sicher die Frage, wie Sie am einfachsten die Einwilligung einholen. Die Art der Einwilligung zum Erhalt von Newslettern oder Werbemails wird in der Praxis über das sogenannte Opt-In eingeholt. Opt-In bezeichnet ein Verfahren, bei dem einem Empfang regelmäßiger E-Mails (z. B. Newsletter) zugestimmt werden muss. Die in der Praxis bewährteste Lösung ist das Anklicken einer Checkbox, neben welcher z. B. folgender Text stehen könnte: „Hiermit erkläre ich mich damit einverstanden, dass folgende Daten, nämlich [genaue Aufzählung] von der XY GmbH zum Zweck der Zusendung von Werbeprospekten über XY-Produkte im Einklang mit der Datenschutzerklärung [URL zu der Erklä-

Q: **Die Mutter unseres Unternehmens sitzt in den USA. Darf ich an sie Personaldaten übermitteln?**

A: „Neben der genauen Zweckdefinierung (bei Konzernen ist das meistens die Matrixstruktur) muss die internationale Datenübermittlung durch eine EU-US Privacy Shield Zertifizierung oder z. B. durch EU-Standardvertragsklauseln gedeckt sein."

Mag. Ines Freitag, CIPP/E (Certified Information Privacy Professional/Europe), Associate CMS

Q: **Inwieweit darf ich Cloud-Services benutzen?**

A: „Neben anderen Voraussetzungen muss vor allem das notwendige vertragliche Regelwerk für Outsourcing (in der Regel EU-Standardvertragsklauseln) gegeben sein."

rung platzieren] verwendet werden. Diese Einwilligung ist freiwillig und kann jederzeit mit Wirkung für die Zukunft gegenüber der XY GmbH unter newsletter@XYGmbH.com widerrufen werden."
Bitte beachten Sie auch, dass die Checkbox nicht per default angehakt sein darf!

Was sonst beim E-Mail Versand zu beachten ist

Wie es die sogenannte Robinsonliste für postalische Werbung gibt, so können Privatpersonen wie Unternehmen ihre E-Mail-Adressen über die ECG-Liste für Werbezusendungen sperren lassen. Dabei handelt es sich um eine von der Regulierungsbehörde für Telekommunikation und Rundfunk (RTR GmbH) geführten Liste, die nur Werbung, die per E-Mail verschickt wird, betrifft. In der Praxis bedeutet die ECG-Liste für Sie als Unternehmen, dass Sie etwaige gesammelte E-Mail-Adressen vor Versand der Werbemail mit dieser Liste abgleichen müssen.

3. Wenn Daten außer Landes gehen

Sitzt die Konzernmutter im Ausland oder haben Sie zum Beispiel die IT an ein Unternehmen jenseits der EU oder des EWR ausgelagert? In diesem Fall gilt es künftig einiges zu beachten.

Grenzüberschreitende Datenübermittlungen gehören mittlerweile zum Alltag – sei es durch die zunehmende Globalisierung oder Konzernbildung oder auch durch kostensparende Auslagerungen von bestimmten Geschäftsprozessen (z. B. IT-Services, Lohnbuchhaltung). Bei der Erstellung des Verarbeitungsverzeichnisses müssen Sie sich auch mit der Frage befassen, wohin Sie die Daten übermitteln. Denn als verantwortliche Stelle bleibt Ihr Unternehmen für die Daten verantwortlich. Auch wenn die Daten ins Ausland gehen, muss Ihr Unternehmen als Übermittler daher sicherstellen, dass die Betroffenendaten ausreichend geschützt sind.

Anhaltspunkte suchen

Suchen Sie in einem ersten Schritt Anhaltspunkte in der bisherigen Dokumentation: Haben Sie z. B. eine Datenbank, in der vermerkt ist, wohin die Daten übermittelt werden? Oder hat Ihr Unternehmen bereits in der Vergangenheit bei der Datenschutzbehörde Meldungen vorgenommen? Verwendet Ihr Unternehmen eine Cloudlösung oder werden die Daten lokal abgespeichert? Sind Sie ein größerer Konzern, der über Tochtergesellschaften oder Niederlassungen außerhalb Österreichs verfügt? Verwenden Sie in Ihrem Geschäftsprozess Lieferanten aus anderen Ländern? Oder verwenden Sie einen externen Wirtschaftsprüfer, der die Lohnbuchhaltung übernimmt und Ihren Mitarbeitern elektronische Gehaltszettel zuschickt? Wird die IT Ihres Unternehmens von der Muttergesellschaft in einem anderen Land gewartet? Ein erster Anhaltspunkt kann dabei auch die Datenschutzerklärung Ihres Unternehmens sein (falls eine vorhanden ist).

Vergessen Sie auch nicht, dass Datenschutz ein betriebsübergreifendes Thema ist: Involvieren Sie daher frühzeitig andere Abteilungen Ihres Unternehmens.

Q: **Ich verschicke seit Jahren Newsletter. Darf ich das künftig noch?**

A: „Ja, wenn es sich dabei um bestehende Kunden handelt, oder die Datenverarbeitung auf wirksamen Einwilligungen und vollständigen Datenschutzerklärungen beruht." Dr. Johannes Juranek, Partner CMS

Was Sie wissen sollten

Ein komplexes Thema ist auch die Bewertung von Datenübermittlungen in sogenannte Drittstaaten. Hierbei handelt es sich um Staaten, die weder der EU angehören, noch zum Europäischen Wirtschaftsraum (Island, Norwegen und Liechtenstein) zählen. Beispiele für solche Drittstaaten sind China, Russland, Indien oder USA.

Zunächst aber die gute Nachricht: Haben Sie einmal festgestellt, wer Ihre Daten bekommt und handelt es sich dabei um Unternehmen in EU- oder EWR-Mitgliedstaaten, ist die Datenübermittlung zulässig, soweit auch der Zweck der Übermittlung gerechtfertigt ist. Dieser Grundsatz gilt auch, wenn Sie Daten in Staaten mit einem angemessenen Datenschutzniveau (welches durch die Europäische Kommission attestiert worden ist) übermitteln. Dabei handelt es sich um Andorra, Argentinien, Kanada, Schweiz, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland oder Uruguay.

Achtung bei USA

Grundsätzlich besteht in den USA kein angemessenes Datenschutzniveau. Um für europäische Geschäftspartner die Datenübermittlung zu erleichtern, wurde zwischen EU und USA das Abkommen „EU-US Privacy Shield" abgeschlossen. Voraussetzung ist, dass sich die Unternehmen mit Sitz in den USA in eine entsprechende Liste eintragen und sich damit selbst zertifizieren. Ihr Unternehmen als Datenübermittler hat im Vorfeld der Übermittlung nur zu überprü-

Erlaubt, wenn …

1.

Daten außer Landes zu schicken ist dann kein Problem, wenn der Empfänger in der EU oder dem EWR sitzt, wozu Norwegen, Island und Liechtenstein zählen, und für die Übermittlung ein berechtigtes Interesse besteht.

2.

Ebenso ist die Datenübermittlung in jene Länder möglich, denen die Europäische Kommission ein angemessenes Datenschutzniveau attestiert. Das sind derzeit Andorra, Argentinien, Kanada, Schweiz, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay. Eine Übermittlung in die USA fällt nur dann unter diese Voraussetzung, wenn der Empfänger eine EU-US Privacy Shield Zertifizierung nachweisen kann.

3.

Für alle anderen internationalen Datenübermittlungen gilt, dass einer der Ausnahmetatbestände wie z. B. der Abschluss von EU-Standardvertragsklauseln oder die Einwilligung des Betroffenen vorliegen muss.

fen, ob das betreffende US-Unternehmen in dieser Liste des US-Handelsministeriums gelistet ist und ob das Ablaufdatum der Zertifizierung noch nicht erreicht ist. Sind diese Voraussetzungen erfüllt, handelt es sich um eine melde- und genehmigungsfreie Übermittlung.

Findet die Datenübermittlung an ein Unternehmen statt, auf das keine der oben genannten Ausnahmen zutrifft, müssen Sie als Datenübermittler sicherstellen, dass der Empfänger dennoch ein angemessenes Datenschutzniveau vorweisen kann. In einem solchen Fall ist es empfehlenswert, die von der EU ausgearbeiteten Standardvertragsklauseln zu verwenden. Dieser Vertrag kann nach der DSGVO grundsätzlich ohne Hinzuziehung der Datenschutzbehörde verwendet werden, wenn Sie ihn in seiner ursprünglichen Form belassen. Werden einzelne Klauseln individuell verändert, bedarf der Vertrag der Genehmigung (wie das nach der derzeitigen Rechtslage auch bei unveränderter Verwendung gilt).

Für die Erstellung des Verarbeitungsverzeichnisses müssen Sie daher die vollständigen Namen und Adressen der Unternehmen, an die Sie Daten übermitteln, aufnehmen. Zusätzlich müssen Sie vermerken, ob Sie die Daten an diese Unternehmen übermitteln, weil Sie sie zur Vertragserfüllung brauchen oder weil Ihnen etwa der Betroffene seine Einwilligung zur Datenweitergabe gegeben hat, etc. Schließlich müssen Sie im Falle von Datenübermittlungen in Drittstaaten die entsprechenden Verträge (z. B. EU-Standardvertragsklauseln) beilegen.

4. Löschen statt horten

Eine Einwilligung zur Verwendung von Daten kann auch widerrufen werden. Die DSGVO räumt daher das Recht des „Vergessen Werdens“ ein: Wie Sie die fristgerechte Datenlöschung im Auge behalten.

Zur Erstellung des Verarbeitungsverzeichnisses gehören auch Angaben zu den Regelfristen für die Aufbewahrung und Löschung der Daten dazu. Dies ist nicht nur für die Datenschutzbehörde bei einer Kontrolle von essenzieller Bedeutung, sondern dient auch der Eigenkontrolle im Unternehmen.

Wie setzen Sie die Datenlöschung praktisch um? Und welche Löschfristen gelten nun? Dazu existieren oft nur unscharfe Formulierungen. Viele Unternehmen beschränken sich daher auf die Aussage, die Daten zu löschen, wenn sie nicht mehr erforderlich sind und verzichten auf konkrete Fristen. Ein solches Vorgehen erschwert nicht nur eine externe Prüfung, sondern legt den Verdacht nahe, dass Sie sich nicht ausreichend mit der Löschung personenbezogener Daten befasst haben. Eine gute Lösung für Ihr Datenmanagement ist, dass Sie Archivfunktionen, Termin-Erinnerungen und Löschfunktionen auf der Datenebene implementieren: Ihr Unternehmen sollte daher sicherstellen, dass den Datenkategorien Speicherfristen zugeordnet werden, welche durch regelmäßig stattfindende Recherchen der zuständigen Abteilung auf ihre Aktualität/Löschung überprüft werden. Es ist auch sinnvoll, sich diese Recherchen mittels elektronischer Terminkalendereinladungen in Erinnerung zu rufen.

Achtung! Mit dem Recht auf „Vergessen Werden“ räumt die DSGVO den Betroffenen das Recht auf unverzügliche Löschung der sie betreffenden Daten ein, wenn sie ihre Einwilligung widerrufen. Damit trifft Ihr Unternehmen nicht nur die Verpflichtung, die Zusendung weiterer Werbemails abzustellen, sondern auch dafür zu sorgen, dass andere verantwortliche Dritte darüber informiert werden. Die Daten müssen dann von Ihnen und verantwortlichen Dritten tatsächlich gelöscht werden.

5. Schätzen Sie Ihr Risiko ein

Unternehmen müssen laut DSGVO selbst beurteilen, ob ihre Datenverarbeitung ein Risiko für die Betroffenen darstellen kann. Ist dies der Fall, ist eine detaillierte Folgenabschätzung vor der Datenverarbeitung notwendig.

Die DSGVO sieht für bestimmte Verfahren die Vornahme einer Datenschutz-Folgenabschätzung („Privacy Impact Assessment") vor. Hinter diesem sperrigen Begriff verbirgt sich die Pflicht der Unternehmen, zunächst einzuschätzen, ob die Datenverarbeitung für die Rechte und Freiheiten der Betroffenen riskant sein könnte: Die Schwierigkeit liegt in der Praxis darin, selbst beurteilen zu müssen, ob in Ihrem Unternehmen ein hohes Risiko besteht. Der Begriff „Risiko" zielt in diesem Kontext aber nicht auf eine wirtschaftliche Betrachtung der Haftungsrisiken ab. Vielmehr geht es um die Frage, ob die Rechte und Freiheiten des Einzelnen betroffen sein könnten (solche Einschnitte in die Persönlichkeitsrechte des Betroffenen werden im Englischen als „Privacy Impact" bezeichnet).

Zusammenfassend impliziert die DSGVO für Unternehmen eine zweistufige Prüfung: In einem ersten Schritt sollten alle Abteilungen Ihres Unternehmens im Rahmen des Datamappings angehalten sein, eine Einschätzung über den „Impact" vorzunehmen. Das heißt sich die Frage zu stellen, ob ein hohes Risiko für die Betroffenen besteht. In einem zweiten Schritt gilt es, die Verarbeitung und die vorzunehmenden Maßnahmen zu beschreiben („Was mache ich genau und was kann ich tun, um das Risiko zu verringern?"). Wie Sie diese Methodik angehen, ist Ihnen von der DSGVO freigestellt.

In der Praxis werden vor allem Unternehmen mit der Vornahme eines Privacy Impact Assessments konfrontiert sein, die neue Technologien (z. B. Tracking Tools) verwenden, mit sensiblen Daten arbeiten (z. B. Pharmaunternehmen) oder die Daten entsprechend der „schwarzen Liste" verarbeiten (dabei handelt es sich um eine Liste von „besonders risikobehaf-

teten“ Datenverarbeitungen, die von der Datenschutzbehörde noch nicht veröffentlicht worden ist).

„Privacy by Default“ und „Privacy by Design“

Diese zwei Wörter sind im europäischen Datenschutzrecht derzeit in aller Munde. Sie spielen im Zusammenhang mit der Modernisierung Ihrer Compliance-Kette und der Implementierung technischer Maßnahmen eine wesentliche Rolle. Den Grundsätzen „Privacy by Default“ und „Privacy by Design“ sollte daher in Ihrem Unternehmen ausreichend Rechnung getragen werden. Mit diesen beiden Trendwörtern schreibt die DSGVO zwei technische Konzepte vor, welche von Ihrem Unternehmen jedenfalls zu beachten und zu implementieren sind: Datenschutz durch Voreinstellungen („Privacy by Default“) und Datenschutz durch Technik („Privacy by Design“). Dass es der EU ernst

CMS entwickelt

DSGVO Helptool

Das CMS DSGVO Helptool ist ein elektronischer Fragebogen, mit dem Sie Angaben zu Ihrer Datenverarbeitung machen können. Die Informationen werden dann von CMS Spezialisten in Form eines schriftlichen Berichts ausgewertet. Auf diese Weise können Sie abschätzen, wie hoch das Risiko in Ihrem Unternehmen ist.

Q: **Wir verschicken unsere Mailings über externe Newsletter-Anbieter. Ist das künftig noch möglich?**

A: „Ja, wenn es sich bei dem Anbieter um einen Auftragsverarbeiter handelt und eine entsprechende Vereinbarung vorliegt. Zusätzlich ist der Betroffene auf die Hinzuziehung von Externen in der Datenschutzerklärung hinzuweisen."

Mag. Ines Freitag, Associate CMS

ist, den Verantwortlichen einer Datenverarbeitung für die Einhaltung dieser Grundsätze in die Verantwortung zu nehmen, zeigen die harschen Strafen, mit welchen Verstöße dagegen sanktioniert werden könnten.

Deshalb sollte Ihr Unternehmen bereits jetzt die entsprechenden datenschutzrechtlichen Vorgaben kennen und durch datenschutzrechtliche Voreinstellungen und durch eine datenschutzgerechte Gestaltung dafür Sorge tragen, dass Sie Daten ohne datenschutzrechtliche Mängel verarbeiten. Um die angemessenen technischen und organisatorischen Maßnahmen durch „Privacy by Default" und „Privacy by Design" zu treffen, bildet das Erstellen des Verarbeitungsverzeichnisses eine wesentliche Voraussetzung. Hat man nämlich einmal die Voraussetzungen für die zulässige Verarbeitung von personenbezogenen Daten verinnerlicht, gestaltet sich die Abwägung, welche „Privacy by-Default" und „Privacy by Design"-Maßnahmen man ergreifen sollte, leichter:

— Dem „Privacy by Default"-Prinzip entsprechend sollte Ihr Unternehmen über eine Website verfügen, die geeignete Privatsphäre-Einstellungen für Ihre Nutzer bereitstellt. Dies kann sich dadurch

Q: **Darf ich eigentlich Whistleblower-Hotlines nutzen?**

A: „Ja. Die Öffnungsklausel der DSGVO verweist dazu auf das neue Datenschutzgesetz, welches eine konkrete Regelung zu den jeweiligen Voraussetzungen trifft." Dr. Johannes Juranek, Partner CMS

äußern, dass im Onlinemarketing-Bereich und einer damit zusammenhängenden Onlinekontoregistrierung dem Nutzer die Möglichkeit gegeben wird, seine erteilte Einwilligung einzusehen und jederzeit zu entziehen. Darüber hinaus ist sicherzustellen, dass die Website über eine Datenschutzerklärung verfügt, welche den Nutzer über die Datenverarbeitung informiert. Auch ist es empfehlenswert, Nutzungsbedingungen/Allgemeine Geschäftsbedingungen entsprechend anzupassen. Letztlich ist ein System zu implementieren, das die Betroffenenrechte (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerruf, Einschränkung der Verarbeitung) sicherstellt. Das könnte z. B. durch die Bereitstellung eines Online-Formulars/einer E-Mail-Adresse zur Kontaktaufnahme geschehen.

— Schließlich ist dem Grundsatz des „Privacy by Design"-Prinzips beispielweise dann Genüge getan, wenn bei einer Datenverarbeitung, die auf einer Einwilligung beruhen soll, die Einwilligung erst dann eingeholt wird, wenn sie tatsächlich benötigt wird und folglich mit der Datenverarbeitung vor Abgabe der Einwilligung nicht begonnen wird.

6. Wie big darf Big Data sein?

Big-Data-Anwendungen spielen im Zuge von Digitalisierung und Industrie 4.0 eine große Rolle. Die DSGVO steckt allerdings den Rahmen ab, inwieweit automatisierte Daten wie etwa Arbeitsleistung oder Aufenthaltsort genutzt werden dürfen.

Das Schlagwort Big Data ist im Zusammenhang mit der Digitalisierung und Industrie 4.0 ein Dauerthema. Big-Data-Anwendungen ermöglichen es, umfangreiche Datenbestände zu erheben, zu speichern, zu verarbeiten und mit anderen Daten zu aggregieren. Auf Basis dieser Auswertungen können die Effizienz der eigenen Geschäftsprozesse oder die Kundenansprachen gesteigert werden. Dieser Datensatz kann aber auch für die automatisierte Entscheidungsfindung genutzt werden, welche es dem Unternehmen ermöglicht, gegenüber den Betroffenen bestimmte Entscheidungen zu treffen. Zur automatisierten Entscheidungsfindung zählt auch das Profiling, welches zur Bewertung persönlicher Aspekte einer natürlichen Person eingesetzt wird: Dabei werden Aspekte wie die Arbeitsleistung, persönliche Vorlieben, Interessen oder Aufenthaltsort analysiert und z. B. als Entscheidungshilfen für Gehaltserhöhungen genutzt.

Im Zusammenhang mit Big Data und Profiling sollten Sie daher beachten, dass für diese Verfahren die allgemeinen Grundsätze der DSGVO gelten (z. B.: Grundsätze der Datensparsamkeit, Zweckbindung und des grundsätzlichen Verbots der Datenverarbeitung vorbehaltlich der Erfüllung eines Erlaubnistat-

bestandes). Zudem sind die besonderen Regelungen zur automatisierten Entscheidungsfindung zu beachten: Sie sehen vor, dass der Betroffene (z. B. der Arbeitnehmer) das Recht hat, nicht ausschließlich einer auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu sein. Ohne Zustimmung ist Profiling unzulässig, wenn die Entscheidung gegenüber dem Betroffenen eine rechtliche Wirkung entfaltet oder in erheblicher Weise beeinträchtigend wirkt. Hierzu zählt unter anderem ein Online-Einstellungsverfahren, Kreditvergaben etc. ohne jegliches menschliches Zutun. Folglich bedarf es im Regelfall menschlicher Intervention. Ausnahmen vom Erfordernis der menschlichen Intervention sind dann gegeben, wenn die automatisierte Entscheidungsfindung für den Abschluss oder die Erfüllung eines Vertrages notwendig ist oder wenn der Betroffene seine Einwilligung gegeben hat.

Pseudonyme können helfen

Für die praktische Umsetzung bedeutet dies, dass Ihr Unternehmen die Überlegung anstellen sollte, ob personenbezogene Daten von vornherein zu Big-Data-Analysen, insbesondere Profiling, genutzt werden. In so einem Fall ist der Einsatz eines angemessenen Pseudonymisierungsverfahrens anzudenken.

7. Hüten Sie sich vor den Strafen

Bei Verstößen gegen die DSGVO drohen Strafen, die wirklich weh tun.

Es bleibt nur noch wenige Monate Zeit, bis die DSGVO in Kraft tritt. Unternehmen drohen dann bei unrechtmäßigen Datenverarbeitungen Strafen: Im Extremfall bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes, je nachdem welcher Wert der höhere ist. Als Bemessungsgrundlage gilt der weltweite Jahresumsatz des vorangegangenen Geschäftsjahres. Von diesem Strafmaß könnte auch Ihr Unternehmen betroffen sein, wenn es nicht frühzeitig die notwendigen Schritte zur Implementierung einer Compliance-Kette setzt.

Wozu die Strafen? Die Sanktionen nach der DSGVO sollen Unternehmen von Datenschutzverstößen abhalten und das Bewusstsein dafür schärfen, dass Verstöße zugleich Verletzungen der europäischen Grundrechte sind. Deshalb sieht es der europäische Gesetzgeber als notwendig an, die Sanktionen wirksam, verhältnismäßig und abschreckend zu gestalten.

Wird die Behörde das volle Strafmaß ausschöpfen? Diese Frage gestaltet sich schwierig, zumal von der österreichischen Datenschutzbehörde bis jetzt keine Stellungnahme zu den Parametern der Höhe der Geldbuße erfolgt ist. Die DSGVO normiert aber eine Reihe an Kriterien (die nicht abschließend sind!), die die Behörde bei der Höhe der Geldbuße heranziehen könnte.

Welche Kriterien sind das? Dabei könnte es sich um die Art, Schwere und Dauer oder die Vorsätzlichkeit bzw. Fahrlässigkeit des Verstoßes handeln. Ebenso könnte die Behörde einschlägige frühere Verstöße oder die Art und Weise, wie der Verstoß der Behörde bekannt wurde (Stichwort „Selbstanzeige") als erschwerenden bzw. mildernden Umstand werten. Ein Kriterium bei der Bemessung kann auch die finanzielle Leistungsfähigkeit des Unternehmens sein.

Welche sonstigen Sanktionen drohen? Die österreichische Datenschutzbehörde könnte auf ihre nach der DSGVO normierten Befugnisse zurückgreifen und Anordnungen zur Beendigung des Verstoßes

Q: **Wer könnte mich überhaupt klagen, wenn ich den Umgang mit Daten nicht so ernst nehme?**

A: „Enttäuschte Mitarbeiter, unzufriedene Kunden oder potenzielle Kunden, aber auch Mitbewerber.“ Dr. Johannes Juranek, Partner CMS

setzen, wie z. B. eine Verwarnung aussprechen oder eine Anweisung, die Datenverarbeitung den Vorgaben der DSGVO anzupassen. Auch ein komplettes Verbot der Datenverarbeitung ist möglich.

Ist das eine abschließende Regelung?
Nein, denn die DSGVO ermöglicht dem nationalen Gesetzgeber weitere Sanktionen einzuführen. So hat der österreichische Gesetzgeber im neuen Datenschutzgesetz, welches auch mit 25. Mai 2018 in Kraft tritt, die Verhängung von Verwaltungsstrafen von bis zu 50.000 Euro vorgesehen. Strafen können auch gegen natürliche Personen, die zur Vertretung der juristischen Person nach außen berufen sind (z. B. Geschäftsführung), verhängt werden!

Wie kommt eine datenschutzrechtliche Compliance-Lücke ans Licht?
Insbesondere in Österreich wird es zu einer Verlagerung der Funktion der Datenschutzbehörde kommen. Die Prüfung des internationalen Datentransfers wird sich einschränken; dafür wird erwartet, dass die Behörde proaktiv Überprüfungen tätigen wird. Auch kann ein unzufriedener Mitarbeiter, der sich bei der Behörde beschwert, ein Verfahren ins Rollen bringen. Oder auch ein Kunde oder die Presse, die für eine Story datenschutzrechtlichen Investigativ-Journalismus betreiben könnte.

Was können Sie tun?
- **Unterschätzen Sie den Datenschutz nicht:** Frühzeitige Sensibilisierung bildet das Fundament für die Implementierung einer Compliance-Kette.
- **Überschätzen Sie sich auch nicht:** Datenschutz ist ein komplexes Thema, und je größer das Unternehmen, desto mehr gibt es zu beachten. Ihr Unternehmen sollte sich daher professionell beraten lassen und regelmäßige Compliance-Audits durchführen.

C/M/S/

Law.Tax

Die DSGVO betrifft auch Sie.

Die Datenschutz-Grundverordnung (DSGVO) betrifft so gut wie alle Unternehmen. Datenschutzverletzungen werden künftig schmerzhaft teuer. Wappnen Sie sich rechtzeitig. Unsere Datenschutz-ExpertInnen sagen Ihnen wie.

Mehr Informationen finden Sie unter
https://cms.law/de/AUT/DSGVO

CMS is an international law firm that helps clients to thrive through technical rigour, strategic expertise and a deep focus on partnerships.

Your World First
cms.law