Experteninterview mit Michael Rohrlich

Rechtsanwalt und zertifizierter Datenschutzbeauftragter TÜV-Süd

Herr Rohrlich, die DSGVO bringt einige Neuerungen und Anforderungen mit sich, die auch kleine Unternehmen und Selbstständige betreffen. Was muss ein Betrieb konkret tun, damit er die DSGVO-Vorgaben umsetzt und Bußgelder vermeidet?

Es gibt verschiedene Maßnahmen, die zu treffen sind. Zunächst einmal sollte im Unternehmen der Ist-Zustand ermittelt werden. Es muss also überprüft werden, ob bereits einzelne Datenschutz-Maßnahmen – von denen es übrigens auch schon nach alter Rechtslage einige gab – im Unternehmen vorhanden sind. Dann muss dieser Ist-Zustand mit dem Soll-Zustand gemäß DSGVO verglichen werden, um erkennen zu können, was nun genau zu tun ist.

Alle Unternehmen mit mehr als 10 Mitarbeitern müssen einen Datenschutzbeauftragten bestellen. Auch kleinere Unternehmen können dazu verpflichtet sein. Das ist dann der Fall, wenn in einem gewissen Umfang besonders sensible Daten verarbeitet werden, wie etwa Gesundheitsdaten oder Informationen über die sexuelle Orientierung. Daher muss beispielsweise ein Zahnlabor mit nur 4 Mitarbeitern auch einen Datenschutzbeauftragten bestellen. Ein existierender Datenschutzbeauftragter muss spätestens ab dem 25.05.2018 der zuständigen Aufsichtsbehörde gemeldet werden.

Wichtig ist auch das Führen des sogenannten Verzeichnisses von Verarbeitungstätigkeiten. Dabei handelt es sich um das zentrale Dokument im Bereich Datenschutz, in dem alle Datenverarbeitungsvorgänge beschrieben und dokumentiert werden. Dieses Verzeichnis muss man der Aufsichtsbehörde auf Nachfrage vorlegen, um so seiner Nachweispflicht nachzukommen.

Dazu gehört auch die Beschreibung der vorhandenen technischen und organisatorischen Maßnahmen, mit denen man im Unternehmen den Datenschutz sicherstellt – z.B. die Zutrittskontrolle im Gebäude, die Sicherung des Serverraums, der Zugang zu Computern mit Kennung und Passwort, eine Firewall, eine Antiviren-Software, aktuelle Betriebssysteme und Anwendungssoftware etc.

Gilt das genauso für kleine Unternehmen oder müssen diese anders vorgehen? Was gilt für 1-Mann-Betriebe?

Die DSGVO gilt prinzipiell auch für kleine Unternehmen und sogar für Einzelunternehmer –unabhängig von Branche, Mitarbeiterzahl, Umsatz oder Organisationsform. Eine Ausnahme existiert nur für den rein privaten Bereich, z.B. die in Excel angelegte Geburtstagsliste von Freunden. Allerdings sieht die DSGVO an manchen Stellen Ausnahmeregelungen für Kleinunternehmen vor. Das gilt etwa für die Pflicht zum Führen des Verzeichnisses von Verarbeitungstätigkeiten. Diese gilt nicht für Unternehmen mit weniger als 250 Mitarbeitern. Allerdings gibt es von dieser Ausnahme auch Gegenausnahmen – z.B. dann, wenn aufgrund der Datenverarbeitung Risiken für die Betroffenen bestehen oder sensible Daten verarbeitet werden. Unter dem Strich lässt sich sagen, dass die eigentliche Ausnahme für Unternehmen mit weniger als 250 Mitarbeitern wohl eher selten greift, so dass im Grunde auch kleinere Unternehmen im Zweifel das Verzeichnis führen sollten.

Welche Bereiche im Unternehmen sind betroffen?

Datenschutz gilt online, aber natürlich auch offline. Daher sind alle Bereiche bzw. Arbeitsabläufe in Unternehmen betroffen, mit denen personenbezogene Daten verarbeitet werden. Nur reine Unternehmensdaten (Bilanz, Statistik etc.) sind ausgenommen. Unter „personenbezogenen Daten" versteht man alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Derjenige, dessen Daten verarbeitet werden, wird „Betroffener" genannt, das datenverarbeitende Unternehmen „Verantwortlicher".

Der Begriff der personenbezogenen Daten wird sehr weit verstanden. Dazu zählen also u.a.:

- persönliche Daten (Name, Anschrift, Geburtsdatum etc.)
- Kontaktdaten (Telefonnummer, Faxnummer, E-Mail-Adresse etc.)
- Finanzdaten (Bankverbindung, Gehaltsabrechnung etc.)
- Fotos mit erkennbar abgebildeten Personen
- Gesundheitsdaten (Krankmeldung, Diagnose, Überweisung etc.)
- Kfz-Kennzeichen
- IP-Adressen

Wenn man sich nicht sicher ist, ob es sich in einem bestimmten Fall um Daten mit Personenbezug handelt, sollte man im Zweifel davon ausgehen, dass dies der Fall ist. Denn es geht hierbei nicht nur um Daten von Kunden, sondern auch um solche von Mitarbeitern, Dienstleistern etc.

Der Begriff der Datenverarbeitung wird ebenfalls sehr weit ausgelegt. Darunter fallen nahezu alle Vorgänge in einem Unternehmen: von der Erhebung über das Organisieren, Speichern, Verknüpfen und Übermitteln bis hin zum Löschen bzw. Vernichten. Im Zweifel sollte man also auch hier davon ausgehen, dass eine bestimmte Tätigkeit unter den Begriff „Verarbeitung von Daten" fällt.

Typische Datenverarbeitungsvorgänge in Unternehmen sind etwa die Bearbeitung einer Bestellung, der Versand eines Newsletters, die Veranstaltung von Gewinnspielen, die Verwaltung von Mitarbeiterdaten oder auch die Verarbeitung von Daten in der Cloud (z.B. Dropbox, Microsoft Office 365 etc.). Ebenso stellen Finanzbuchhaltung, Urlaubsplanung, Reisekostenabrechnung oder Bewerbermanagement relevante Datenverarbeitungsvorgänge dar.

Müssen Unternehmen ihre bestehenden Datenschutzerklärungen erweitern? Wenn ja, wie bzw. um welche Punkte?

Wer eine nicht nur rein private Internetseite betreibt, muss neben einem Impressum auch eine Datenschutzerklärung bereitstellen. Dies war bislang schon so und wird sich auch unter der DSGVO nicht ändern. Allerdings müssen die Inhalte an die neue Rechtslage angepasst werden. Nach Maßgabe der DSGVO müssen Website-Besucher beispielsweise über Namen und Kontaktdaten des Unternehmens, einen eventuell vorhandenen Datenschutzbeauftragten, die Zwecke der Datenverarbeitung und deren Rechtsgrundlage, die Dauer der Datenspeicherung, die Betroffenenrechte (auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenportabilität) oder auch über das Beschwerderecht bei Aufsichtsbehörden informiert werden. Insbesondere müssen auf der Internetseite eingesetzte Technologien, wie z.B. Cookies, Analysesoftware, Werbung, Social Plugins, Kontaktformulare etc., im Rahmen der Datenschutzerklärung näher beleuchtet werden.

Was muss man konkret beachten, wenn man Werbung (Briefe/ E-Mailings) versenden möchte?

Bei dem Versand von Werbung ist zu unterscheiden, ob diese per Brief oder auf elektronischem Wege, also z.B. per E-Mail, verschickt wird. Beim postalischen Versand gilt das sogenannte Opt-Out-Prinzip. Das heißt: Es darf so lange Werbung verschickt werden, bis der Empfänger dem widerspricht. Beim elektronischen Versand ist es genau anders herum: Hier muss der Empfänger vorab ausdrücklich dem Erhalt von Werbe-E-Mails zustimmen, sonst darf kein Versand erfolgen. Da es diese Regelungen auch schon vor Inkrafttreten der DSGVO gab, wird sich in dieser Hinsicht nichts ändern.

Folgende Punkte sind beim E-Mail-Marketing zu beachten:

- Vollständige E-Mail-Signatur inkl. aller wichtigen Unternehmensangaben (vgl. Impressum)
- deutlicher Hinweis auf Werbung schon in der Betreffzeile
- keine unlauteren Inhalte (also korrekte Produktbeschreibungen, Preisangaben etc.)
- Beachtung der Datensparsamkeit (nur E-Mail-Adresse als Pflichtangabe erheben)
- Beachtung des Double-Opt-In-Prinzips (Versand erst nach Erhalt der Einwilligung und erfolgreicher Verifizierung der Mail-Adresse)

Wie hoch ist die Wahrscheinlichkeit, dass kleine Unternehmen wirklich kontrolliert werden?

Das ist schwer zu beantworten. Es ist so, dass wohl alle Datenschutzaufsichtsbehörden in Deutschland vermehrt Personal eingestellt haben, um ihren neuen Aufgaben nachkommen zu können. Aber sicherlich gibt es auch jetzt nicht so viele Mitarbeiter, dass alle Unternehmen aktiv kontrolliert werden können. Vermutlich werden zunächst einmal – wenn überhaupt – eher größere Unternehmen Ziel der Aufsichtsbehörden sein.

Aber sicherlich werden auch bei mittleren und kleineren Unternehmen stichprobenartige Kontrollen durchgeführt werden. Zudem lässt sich manches auch automatisiert erledigen, wie etwa die Überprüfung der Online-Datenschutzerklärung oder die Pflicht zur Meldung eines Datenschutzbeauftragten. Es kann auch sein, dass die Aufsichtsbehörden die Unternehmen in ihrem Zuständigkeitsgebiet anschreiben, die keinen Datenschutzbeauftragten gemeldet haben, nach Information der Behörde aber eigentlich einen solchen benennen müssten.

Mit welchen Strafen müssen kleine Unternehmen rechnen, wenn sie die Vorgaben nicht umsetzen? Drohen wirklich auch kleinen Unternehmen Bußgelder in Millionenhöhe?

Bei den Sanktionen macht die DSGVO grundsätzlich keinen Unterschied zwischen großen, mittleren oder kleinen Unternehmen. Je nach Verstoß stehen daher für alle gleichermaßen bis zu 10 Millionen Euro bzw. bis zu 20 Millionen Euro Geldbuße im Raum. Früher lag die Grenze bei 50.000 bzw. 300.000 Euro. Bußgelder sollen prinzipiell „wirksam, verhältnismäßig und abschreckend“ sein. Allerdings gibt es diverse Kriterien, die bei der Bemessung des konkreten Betrages zu beachten sind.

Dazu zählen u.a. folgende Aspekte:

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung von Art, Umfang oder Zweck der betreffenden Verarbeitung sowie der Zahl der Betroffenen und des Ausmaßes des erlittenen Schadens
- vorsätzliche oder fahrlässige Begehung
- vom Unternehmen getroffene Maßnahmen zur Minderung des Schadens
- eventuell einschlägige frühere Verstöße des Unternehmens
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und mögliche nachteilige Auswirkungen zu mindern
- Kategorien der betroffenen Daten
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und ggf. in welchem Umfang das Unternehmen den Verstoß mitgeteilt hat
- jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall (z.B. unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste)

Insgesamt wird ein internationaler Konzern daher ein viel höheres Bußgeld zahlen müssen, als ein kleiner Handwerksbetrieb oder ein mittelständisches produzierendes Unternehmen mit 30 Mitarbeitern. Doch die Sanktionen werden wohl für alle spürbar ausfallen, da sich Datenschutzverstöße nicht mehr „lohnen“ sollen.

Wird es eine Schonfrist geben, in der noch keine Bußgelder verhängt werden?

Auch das ist nicht leicht zu beantworten. Generell ist es so, dass die DSGVO bereits im Mai 2016 in Kraft getreten ist und eine zweijährige Übergangsfrist vorsieht. Daher entfaltet sie ihre volle Wirkung zum 25.05.2018. Ab dann müssen alle Anforderungen umgesetzt sein, das Gesetz sieht keine weitere Übergangsfrist vor. Ob und wann die Behörden die ersten Maßnahmen ergreifen, ist noch nicht ganz klar. Allerdings hat schon die eine oder andere Behörde angekündigt, nicht allzu lange nach dem Stichtag abzuwarten und die Unternehmen in ihrem Bundesland zeitnah anzuschreiben. Es ist also besser, schon mal mit der Umstellung auf die DSGVO anzufangen, auch wenn man nicht bis zum 25.05.2018 damit 100%-ig fertig wird. Denn das ist allemal besser, als noch gar nichts unternommen zu haben.

Rechtsanwalt Michael Rohrlich

www.ra-rohrlich.de