Datenschutz: Alle Hausaufgaben erledigt?

Wenn mit dem 25. Mai 2018 die Datenschutzgrundverordnung (DSGVO) in Kraft tritt, sollten alle Unternehmen ihre Datenanwendungen an die neue Rechtslage angepasst haben. Sobald personenbezogene Daten verarbeitet werden, z. B. für eine Kundenkartei, zum Ausstellen von Rechnungen oder für Informationen über Lieferanten, muss man sich mit den Neuerungen der DSGVO auseinandersetzen.

Mag. Jakob Hütthaler-Brandauer, Rechtsberater der IGEPHA, nahm zu einigen Aspekten der Datenschutzgrundverordnung Stellung:

Welche Maßnahmen sind hinsichtlich der Verarbeitung personenbezogener Daten zu treffen, wenn ein OTC-Unternehmen mit einer Apotheke eine Geschäftsbeziehung hat, z. B. weil Produkte direkt an die Apotheke geliefert werden?

Mag. Hütthaler-Brandauer: Die DSGVO kennt zur Frage, ob eine Datenverarbeitung rechtmäßig – das heißt zulässig – ist, in ihrem Art. 6 insgesamt sechs verschiedene Voraussetzungen. Eine davon ist die Notwendigkeit, die Daten zur Erfüllung vertraglicher oder vorvertraglicher Pflichten zu verarbeiten. Im Rahmen einer Geschäftsbeziehung zu einem Vertragspartner können daher dessen Daten, welche zur Durchführung der vertraglichen Beziehung notwendig erscheinen, verarbeitet werden. Darunter fallen beispielsweise somit auch die personenbezogenen Daten von Ansprechpersonen in der Apotheke.

Betrifft die Geschäftsbeziehung automatisch alle in der Apotheke beschäftigten Personen – Apothekenleiter und alle Angestellten?

Mag. Hütthaler-Brandauer: Nein, das ist nicht der Fall. Es gilt, dass nur jene Daten verarbeitet werden dürfen, die für den Zweck auch notwendig sind. Es bedarf dazu nicht der Daten aller Mitarbeiter, sondern eben nur jener, die für die Vertragsabwicklung nötig sind.

Müssen von allen Personen, deren Daten bereits vor dem 25. Mai 2018 verarbeitet wurden, erneut Einwilligungserklärungen vorgelegt werden?

Mag. Hütthaler-Brandauer: Entsprechen die vorliegenden Einwilligungserklärungen bereits den aktuellen Anforderungen des Datenschutzrechts, müssen diese nicht erneut eingeholt werden. Der Verantwortliche muss dies aber nachweisen können. Liegen aber weder eine rechtskonforme Willenserklärung noch ein anderweitiger Grund für die Rechtmäßigkeit gemäß Art. 6 DSGVO vor, ist die Datenverarbeitung unzulässig.

Was ist generell hinsichtlich jener Daten zu tun, die vor dem 25. Mai 2018 gesammelt und verarbeitet wurden?

Mag. Hütthaler-Brandauer: Im Rahmen der Umsetzung der neuen Verpflichtungen sollten sämtliche Daten gesichtet werden. Es sollte geprüft werden, ob eine Berechtigung zur Verarbeitung entsprechend der DSGVO besteht, beispielsweise durch das Vorliegen einer Einwilligungserklärung oder der Notwendigkeit zur Vertragserfüllung. Dabei sollte auch geprüft werden, ob man alle Daten auch tatsächlich benötigt oder ob man überschießend Daten erhoben und gespeichert hat. Im Rahmen der DSGVO gilt unter anderem nämlich der Grundsatz der Datenminimierung. Die Datenverarbeitung soll dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Brauchen OTC-Unternehmen einen Datenschutzbeauftragten?

Mag. Hütthaler-Brandauer: Die DSGVO beinhaltet leider eine ganze Reihe unbestimmter Begriffe, so auch beim Datenschutzbeauftragten. Ein Datenschutzbeauftragter ist nach Art. 37 unter anderem dann erforderlich, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Was aber genau unter Kerntätigkeit zu verstehen ist, besagt die Verordnung nicht. Meines Erachtens bedarf ein OTC-Unternehmen, das keine sensible Daten verarbeitet, keines Datenschutzbeauftragten, da sonst jedes Unternehmen einen Datenschutzbeauftragten benötigen würde.

Eine zweite Voraussetzung wäre, dass die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung sensibler Daten besteht. Dazu zählen z. B. Gesundheitsdaten. Verarbeitet also ein OTC-Unternehmen personenbezogene Gesundheitsdaten, ist jedenfalls eine genauere Prüfung, ob ein Datenschutzbeauftragter notwendig ist, erforderlich.

Welche sensiblen Daten könnten in OTC-Unternehmen typischerweise verarbeitet werden?

Mag. Hütthaler-Brandauer: Das sind jedenfalls gesundheitsbezogene Daten. Darunter fallen nicht nur Krankheiten einer Person, sondern sämtliche Daten, die irgendwie mit der Gesundheit einer Person zusammenhängen. Darunter zu verstehen sind auch genetische sowie biometrische Daten oder Daten zum Sexualleben.

Was sollte dabei besonders beachtet werden?

Mag. Hütthaler-Brandauer: Die Verarbeitung sensibler Daten ist nach Art. 9 DSGVO grundsätzlich verboten. Abweichungen gelten nur in den von der DSGVO definierten Fällen. Dazu zählt beispielsweise, dass die betroffene Person der Verarbeitung zu festgelegten Zwecken ausdrücklich zugestimmt hat oder die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

Welche Maßnahmen müssen ergriffen werden, um Abonnenten von Newslettern bzw. Besucher von Firmen-Websites, Webshops und Apps über ihre Rechte zu informieren?

Mag. Hütthaler-Brandauer: Jedem Unternehmen ist zu raten, eine Datenschutzerklärung zu verfassen. Diese kann auf einer Website, im Newsletter oder im Webshop gezeigt werden und soll die betroffene Person darüber aufklären, wie das Unternehmen mit personenbezogenen Daten umgeht. An dieser Stelle kann bereits auf die Rechte der betroffenen Person (Betroffenenrechte) hingewiesen werden. Darunter zu verstehen sind das Auskunftsrecht, das Recht auf Berichtigung, das Recht auf Löschung („Recht auf Vergessenwerden"), das Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit und das Widerspruchsrecht.

Außerdem muss die betroffene Person darüber informiert werden, wenn die Erhebung von personenbezogenen Daten bei der betroffenen Person erfolgt oder wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.

Welche neuen Verpflichtungen kommen auf die Personalverwaltung zu? Müssen von allen Mitarbeitern Einwilligungserklärungen eingeholt werden?

Mag. Hütthaler-Brandauer: Grundsätzlich nein, weil die Verarbeitung von Mitarbeiterdaten zur Erfüllung der Verpflichtung aus dem Arbeitsverhältnis erforderlich ist. Beachtet werden muss aber dabei, ob man wirklich alle Daten, die man von einem Mitarbeiter hat, auch wirklich benötigt.

Wie lange darf man Bewerbungen von Personen, die nicht eingestellt wurden, in Evidenz halten?

Mag. Hütthaler-Brandauer: Es ist erneut auf den Grundsatz der Datenminimierung hinzuweisen, wonach die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Der Zweck der Verarbeitung von Bewerbungen wird konsequenterweise mit Beendigung des Bewerbungsprozesses erfüllt sein und auch die betroffene Person wird vermutlich bis zu diesem Zeitpunkt in die Verarbeitung ihre Einwilligung erteilt haben. Eine darüberhinausgehende Verarbeitung erfordert einen Grund für die Rechtmäßigkeit gemäß Art. 6 DSGVO. Liegt dieser nicht vor (etwa die Zustimmung, die Daten für allfällige zukünftige freie Stellen zu verwahren in Kombination mit der Angabe einer Aufbewahrungsdauer), müssen die Daten gelöscht werden.

Welche Quellen empfehlen Sie für die vertiefende und weiterführende Information über die DSGVO?

Mag. Hütthaler-Brandauer: Sowohl im Internet als auch in Form von Büchern gibt es zahlreiche, auch praxisnahe Informationen. Oder Sie fragen Ihren Rechtsberater.