Die größten Datenschutz-Mythen

Im Mai 2018 traten die neuen Datenschutzregeln der Europäischen Union in Kraft. Die Datenschutz-Grundverordnung (DSGVO) führte in vielen Unternehmen zu Verwirrung und Verunsicherung – und viele verstehen die neuen gesetzlichen Vorschriften zum Datenschutz bis heute nicht oder nicht richtig.

Um die neue DSGVO ranken sich viele Mythen, die den Unternehmen in der praktischen Anwendung das Leben schwer machen. Mit diesen Irrtümern soll nachfolgend aufgeräumt werden.

Foto: Tomasz Zajda - stock.adobe.com

Irrtümer aus dem ersten Jahr

Mythos 1: Jede Datenerfassung bedarf einer Einwilligung

Diese Einschätzung ist schlichtweg unzutreffend. Die Datenverarbeitung ist grundsätzlich auch ohne eine Einwilligung erlaubt, wenn ein berechtigtes Interesse an der Datenverarbeitung vorliegt und schutzwürdige Interessen des Betroffenen (insbesondere von Kindern) dem nicht entgegenstehen. Außerdem ist keine Einwilligung notwendig, wenn die Datenverarbeitung insbesondere erforderlich ist

- zur Erfüllung eines Vertrags,
- für vorvertragliche Maßnahmen auf eine Anfrage hin,
- zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen.

Mythos 2: Kunden dürfen öffentlich nicht mit Namen angesprochen werden

Diese Einschätzung ist ebenfalls unzutreffend. Natürlich kann beim Empfang ein Mitglied oder Kunde nach wie vor mit seinem Namen angesprochen werden. Die Zielsetzung der DSGVO sieht keineswegs eine solche Einschränkung vor.

Mythos 3: Rechnungen müssen nach drei Monaten gelöscht werden

Wenn diese Auffassung zutreffend wäre, würde das Unternehmen, das die Daten löscht, erhebliche Schwierigkeiten mit dem Finanzamt bekommen. Nach wie vor gelten die handels- und steuerrechtlichen Aufbewahrungsfristen. Daran haben auch die datenschutzrechtlichen Vorschriften der DSGVO nichts geändert.

Mythos 4: E-Mails dürfen in Firmen nicht weitergeleitet werden

Eine solch pauschale Aussage ist ebenso unzutreffend. Hierbei ist allerdings im Einzelfall zu prüfen, wer innerhalb eines Unternehmens welche personenbezogenen Daten tatsächlich erhalten soll oder nicht. Ein pauschaler Ausschluss der Weiterleitung von E-Mails sieht die DSGVO allerdings nicht vor.

Mythos 5: Wer Menschen fotografiert, muss immer eine schriftliche Einwilligung von allen einholen

Diese Einschätzung ist unzutreffend. Allerdings ist zu bemerken, dass es für ein Unternehmen sinnvoll erscheint, jedenfalls dann von den Mitarbeitern Einwilligungserklärungen einzuholen, wenn sie mit einem Foto auf der Website des Unternehmens gezeigt werden sollen.

Mythos 6: Unternehmen dürfen nur per verschlüsselter E-Mail kommunizieren

Auch diese Vorgabe ist in der DSGVO nicht vorgesehen. Allerdings kann es sich im Einzelfall anbieten, im Unternehmen entsprechende Verschlüsselungssysteme einzuführen, die die E-Mail-Korrespondenz als solches sicherer machen.

Mythos 7: Alle alten Adresslisten müssen gelöscht werden

Im Zusammenhang mit dem Inkrafttreten der DSGVO haben viele Unternehmen ihre alten Adressdaten vollständig gelöscht. Ein solcher Schritt war in vielen Fällen unnötig, denn die DSGVO sieht auch eine solche pauschale Löschung alter Daten nicht vor. Allerdings sollte das Unternehmen überprüfen, wie sich die Altdatenbestände tatsächlich zusammensetzen. Bei früheren Geschäftspartnern und Kunden, mit denen man seit vielen Jahren keinen Kontakt mehr pflegt, ist in der Tat zu klären, ob

Info

Matthias W. Kroll hat auf der diesjährigen 8. IFAA Solutions in Wiesbaden zu den Themen „Resümee aus einem Jahr Datenschutzverordnung“ und „Die häufigsten Fehler in der Personalarbeit und wie Sie diese vermeiden“ referiert.

hier nicht gegebenenfalls doch die Löschung der Daten erforderlich ist.

Mythos 8: Die DSGVO verbietet die Datenübermittlung in die USA

In der Tat ist es so, dass die USA grundsätzlich nicht das identische Datenschutzniveau haben wie die Europäische Union unter der DSGVO. Wenn Daten aus der EU in die USA übermittelt werden sollen, ist für ein deutsches Unternehmen zu beachten, dass sich die Unternehmen mit Sitz in den USA in eine entsprechende Liste des US-Handelsministeriums eingetragen haben. Außerdem müssen sie sich verpflichtet haben, die durch das Abkommen „Privacy Shield“ definierten Garantien und Beschränkungen einzuhalten.

Mythos 9: Jedes Unternehmen muss einen Datenschutzbeauftragten haben

Eine solche Verpflichtung ist oftmals im Zusammenhang mit dem Inkrafttreten der DSGVO insbesondere von Beratern behauptet worden – jedoch existiert eine solche Verpflichtung tatsächlich nicht. Die Voraussetzungen für ein Unternehmen, einen Datenschutzbeauftragten bestellen zu müssen, sind klar geregelt. Sie hängen von der Größe des Unternehmens und von der Art und Weise der Verarbeitung besonderer personenbezogener Daten ab.

Bilanz nach einem Jahr

Was ist in einem Jahr DSGVO tatsächlich passiert? Die Datenschutzaufsichtsbehörden in Europa haben sich im Wesentlichen zunächst erst einmal die großen Unternehmen vorgenommen: So hat die französische Datenschutzbehörde CNIL Google mit einer Geldbuße von 50 Millionen Euro wegen diverser Verstöße gegen die DSGVO belegt. Für Google sind damit diese Bußgelder höher als deren Steuerlast.

Aber auch kleinere und mittlere Unternehmen sind verstärkt in den Fokus der Datenschutzaufsicht geraten. So hat der Landesdatenschutzbeauftragte des Landes Baden-Württemberg mit 80.000 Euro bislang die höchste Einzelgeldbuße verhängt. In diesem konkreten Fall ging es darum, dass ein Unternehmen aufgrund unzureichender interner Kontrollmechanismen Gesundheitsdaten ins Internet gestellt hatte, die für Dritte ohne Weiteres zugänglich waren.

Die Datenschutzaufsicht in Hamburg verhängte insgesamt Bußgelder in Höhe von 25.000 Euro, dabei in einem Fall ein Bußgeld in Höhe von 5.000 Euro für das Fehlen eines Auftragsverarbeitungsvertrages. In Nordrhein-Westfalen sind durch die Landesdatenschutzbehörde Bußgelder in Höhe von ca. 15.000 Euro verhängt worden. Nach Auskunft des Bayerischen Landesamtes für Datenschutzaufsicht wurden im Jahr 2019 2.500 Datenpannen gemeldet und derzeit laufen bereits dort 85 Bußgeldverfahren wegen Verletzung der Datenschutz-Grundverordnung. Auch in den anderen Bundesländern zeigt sich ein ähnliches Bild.

Ausblick: Womit ist in Zukunft zu rechnen?

Der Baden-Württembergische Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) Stefan Brink hat es wie folgt formuliert: „2019 wird das Jahr der Kontrollen. Wer auf Lücke setzt, der muss damit rechnen, dass 2019 ein schwieriges Jahr wird.“

Datenschutz ist in hohem Maße an die aktuellen technischen Standards gekoppelt. Was also vor einem Jahr noch ausreichend war, kann heute bereits schon ungenügend sein. Als Unternehmen darf man sich daher diesen Änderungen nicht versperren und muss ständig überprüfen, ob die Maßstäbe der Datenschutz-Grundverordnung eingehalten werden. Eine solche gesetzliche Verpflichtung sieht die Datenschutz-Grundverordnung in Art. 5 Abs. 2 DSGVO auch selbst vor.

Was müssen Sie als Unternehmer tun?

1. „Dranbleiben“

Datenschutz unter der DSGVO ist ein dynamischer Prozess, der nach Abschluss einer Implementierung eines Datenschutzmanagementsystems nicht endet. Deshalb hat man als Geschäftsführer oder als Geschäftsführerin eines Unternehmens die regelmäßige Verpflichtung, die Anforderungen der Datenschutz-Grundverordnung zu überprüfen und anzupassen.

2. Auditieren

Soweit ein Unternehmen ein Datenschutzmanagementsystem implementiert hat, sollten regelmäßige Audits durch externe Dienstleister durchgeführt werden. Damit sind auch sogenannte Penetrationstests gemeint, also etwa die Überprüfung, ob mit Auskunftsanfragen oder Löschungsbegehren ordnungsgemäß im Unternehmen umgegangen wird und die jeweiligen implementierten Prozessabläufe tatsächlich funktionieren.

3. Eigene Standards aktualisieren

Wenn etwa neue Verarbeitungsprozesse im Unternehmen entstanden sind, so sind diese neuen Verarbeitungsprozesse auch in das Verarbeitungsverzeichnis aufzunehmen. Montiert z.B. ein Unternehmen neue Überwachungskameras, handelt es sich hierbei um einen weiteren Verarbeitungsprozess, der datenschutzrechtlich in das Verarbeitungsverzeichnis aufgenommen werden muss.

Darüber hinaus ist es auch mit Blick auf die bereits erteilten Bußgelder sinnvoll, die Liste der Auftragsverarbeiter nach Aktualität zu überprüfen. Ebenso sind die sogenannten Technischen und Organisatorischen Maßnahmen (TOMs) an aktuelle technische Entwicklungen anzupassen. Matthias W. Kroll

Matthias W. Kroll, LL.M., ist Rechtsanwalt, Fachanwalt für Arbeitsrecht und Fachanwalt für Versicherungsrecht in der Rechtsanwaltskanzlei Dr. Nietsch & Kroll, Hamburg. Er berät Unternehmen der Fitnessbranche in allen rechtlichen Fragen, wie z.B. sozialversicherungsrechtliche, arbeitsrechtliche, haftungs-, versicherungs- und immobilienrechtliche oder AGB-rechtliche Fragen. Zudem ist er zertifizierter Datenschutzbeauftragter des TÜV und betreut Unternehmen bei der Einführung von Datenschutzmanagementsystemen nach neuem Datenschutzrecht. Kontakt: www.nkr-hamburg

Foto: Matthias Kroll