DAS ENDE DER SCHLAMPIGEN VERHÄLTNISSE

Die Datenschutzklippe naht

Den 25. Mai 2018 sollte sich wohl jeder Unternehmer in der EU im Kalender rot einkringeln. Denn an diesem Tag tritt die neue Datenschutz Grundverordnung der EU (EU-DSGVO) in Kraft. Damit wird der Datenschutz personenbezogener Daten innerhalb der EU auf eine neue, einheitliche und vor allem recht anspruchsvolle Basis gestellt. Neu ist auch die geregelt Durchsetzung sowie die drakonisch verschärften Strafen

TEXT: Dominik Schebach | **FOTO:** Pixelio, Fabasoft | **INFO:** www.elektro.at

Jedes Unternehmen arbeitet mit Daten – Rechnungsdaten oder Unternehmensdaten, Kundendaten oder die Daten von Mitarbeitern. Dabei ist es unerheblich, ob es sich um einen Handelsbetrieb mit Online-Shop oder ein Installationsunternehmen dreht. Ohne Daten geht es heute nicht mehr, überall fallen Daten an. Und das ist auch schon die Crux bei der Sache. Denn die viele Unternehmen haben ihre Datenbestände nicht vollständig unter Kontrolle noch lassen sich die personenbezogenen Daten zentral verwalten oder wurde die Datenerfassung dokumentiert.

Aber diese schlampigen Verhältnisse im Bezug auf personenbezogenen Daten haben ein hartes Ablaufdatum. Denn die bereits im Jahr 2016 beschlossene Datenschutz Grundverordnung der EU stellt diese personenbezogenen Daten ab kommenden Jahr unter besonderen Schutz – und dies gilt für alle Staaten der EU und für alle in der EU tätigen Unternehmen. Dh, die neue EU-DSGVO betrifft Amazon und Google ebenso wie den regionalen Elektrohändler mit eigenem Online-Shop. Und wenn man sich auch selbst vielleicht nicht direkt betroffen sieht, wer mit Partnern oder Behörden zusammenarbeitet und Daten austauscht, wird mit dem neuen Datenschutzgesetz in Berührung kommen.

„Ab dem 25. Mai 2018 wird die Datenschutzgrundverordnung DSGVO die neue harte Realität im Datenschutzrecht sein“, erklärte deswegen auch Dr. Rainer Knyrim, von der ersten auf Datenschutzrecht spezialisierten österreichischen Anwaltskanzlei Knyrim Trieb Rechtsanwälte, bei einer gemeinsamen Veranstaltung mit dem österreichschen Software-Unternehmen Fabasoft vor Journalisten.

Mit der EU-DSGVO und dem damit einhergehenden neuen Datenschutzrecht werden alle personenbezogenen Daten innerhalb der EU unter einen besonderen Schutz gestellt. Gestärkt werden vor allem die Rechte von Privatpersonen, womit auch auf alle Unternehmen neue Verpflichtungen zukommen.

GRUNDLEGENDES

Sieht man sich die DSGVO an, so fallen unmittelbar zwei grundlegende Änderungen auf: Die Aufwertung der Datenschutzbehörde und die Anhebung der Strafen. Waren in der Vergangenheit maximal 25.000 Euro bei Verstößen gegen das Datenschutzgesetz fällig, so liegt in Zukunft die Höchststrafe bei 20 Mio Euro bzw 4% des globalen Umsatzes eines Unternehmens – je nachdem was höher liegt. Auch große Konzerne werden es sich unter diesen Umständen zwei Mal überlegen, ob sie eine Übertretung riskieren.

Beauftragt mit der Durchsetzung der Verordnung sind in Zukunft die nationalen Datenschutzbehörden. In Österreich erhält die Behörde dazu neue Befugnisse. Mussten die Datenschützer in der Vergangenheit bei Übertretungen ein Unternehmen bei der Bezirksbehörde anzeigen, so können sie nun selbst tätig werden, Unternehmen (nach Ankündigung) vor Ort kontrollieren, und unter anderem auch bei Gefahr in Verzug direkt die Einstellung von Tätigkeiten anordnen oder im Extremfall Server beschlagnahmen.

SECHS PRINZIPIEN

Inhaltlich beruht die neue DSGVO auf wenigen Prinzipien. Nach diesen richtet sich das gesamte weitere Regelwerk aus. So dürfen laut EU-DSGVO die persönlichen Daten nur ...

1. rechtmäßig und fair gewonnen werden (Grundsatz der Rechtmäßigkeit,

AM PUNKT

EU-DSGVO
tritt mit 25. Mai 2018 in Kraft. Das dazugehörige österreichische neue Datenschutzgesetz wurde Ende Juni im Nationalrat beschlossen.

GESTÄRKT
Die Rechte von Privatpersonen werden damit deutlich gestärkt, gleichzeitig wird die Datenschutzbehörde neu aufgestellt und die Strafen deutlich erhöht.

Verarbeitung nach Treu und Glauben, sowie Transparenz).

2. für die zuvor festgelegten Zwecke verwendet werden (Zweckbindung).

3. nur für den Zweck der Verarbeitung notwendige Maß beschränkt gespeichert werden („Datenminimierung").

4. nur sachlich richtig gespeichert und müssen erforderlichenfalls auf dem neuesten Stand gebracht werden (Richtigkeit).

5. nur solange – in einer Form, die die Identifizierung der betroffenen Person erlaubt – gespeichert werden, wie es für die zweckgebundene Nutzung notwendig ist (Speicherbegrenzung).

6. nur in so einer Form gespeichert werden, die eine angemessene Sicherheit der Daten gewährleistet (Integrität und Vertraulichkeit).

Die im Unternehmen für die Einhaltung dieser Grundprinzipien verantwortlichen Mitarbeiter müssen zudem die Einhaltung des EU-DSGVO nachweisen können.

Viele dieser Grundprinzipien sind derzeit eher vage gehalten, denn die EU hat die Ausgestaltung der Verordnung hier den Mitgliedsstaaten überlassen. Das entsprechende neue Datenschutzgesetz wurde Ende Juni im Nationalrat beschlossen. „Im Unterschied zur EU-DSGVO ist das Datenschutz-Anpassungsgesetz 2018 klarer formuliert, wobei man der praktischen Umsetzung vieler Verpflichtungen noch mit Spannung entgegensehen muss", wie auch Knyrim erklärte. Für Unternehmen heißt dies, dass sie nur noch zehn Monate Zeit haben, um alle Prozesse der personenbezogenen Datenverarbeitung auf die Bestimmungen der neuen EU-DSGVO bzw des neuen Datenschutzgesetzes abzuklopfen und dementsprechend anzupassen.

Das bedeutet, dass die Unternehmen nun einmal alle Prozesse durchleuchten müssen, ob sie der neuen Rechtslage entsprechen. Nach Einschätzung von Knyrim sollten hier Unternehmen, die schon bisher „sauber" mit den Daten ihrer Kunden, Lieferanten und Mitarbeiter umgegangen sind, geringere Probleme haben.

ANPASSUNGSBEDARF

Anpassungsbedarf wird es allerdings dennoch geben. Das beginnt schon mit dem Sammeln der Daten (Punkt 1). Hier ist praktisch alles, dem der Kunde nicht explizit zustimmt, verboten. Kritisch ist auch die Zweckbindung (Punkt 2). Viele Unternehmen besitzen heute einen Datenpool von personenbezogenen Daten, der über Jahre angesammelt wurde – und das meistens ohne Dokumentation bezüglich des Zwecks.

Besondere Herausforderungen ergeben sich auch aus den Anforderungen zur Datenminimierung, Speicherbegrenzung, Vertraulichkeit und Richtigkeit. So dürfen nur die Daten erfasst werden, welche für den Geschäftsfall wirklich benötigt werden. Auch muss das Unternehmen sicherstellen, dass diese Daten richtig sind – kritisch wird das zB bei Bonitätsdaten, die einmal in der Kartei nie mehr kontrolliert werden. Werden die Daten nicht mehr benötigt, weil zB das Geschäft abgeschlossen wurde und die rechtliche Behaltefrist ausgelaufen ist, muss es auch einen Prozess zur planmäßigen Löschung solcher Daten geben. Und die Sicherheit der Daten muss gewährleistet sein.

DIE ZEIT DRÄNGT

Besonders der letzte Punkt dürfte viele Unternehmen vor große Herausforderungen stellen. Zumal in vielen Unternehmen es derzeit keine einheitliche Vorgaben gibt, wie mit persönlichen Daten umgegangen wird, und die Daten dezentral über viele Computer (Buchhaltung, Marketing, Service usw) verteilt gespeichert sind. Damit wird aber eine Verwaltung der Daten sowie eine Erfüllung der Dokumentationspflichten gemäß der EU-DSGVO praktisch unmöglich. Aber auch der Austausch von personenbezogenen Daten per E-Mail oder der Zugriff von externen Partnern auf die Datenbestände eines Unternehmens sind unter diesen Umständen höchstproblematisch. Angesichts der Tatsache, dass IT-Projekte sich oft lange hinziehen, kann man sich also nicht früh genug mit der EU-DSGVO beschäftigen. ■

„Ab dem 25. Mai 2018 wird die Datenschutzgrundverordnung DSGVO die neue harte Realität im Datenschutzrecht sein", erklärte Datenschutzexperte Dr. Rainer Knyrim.

EIN KRITISCHER BLICK AUFS UNTERNEHMEN

Mit dem neuen Datenschutz muss man nicht sofort seine ERP-Software auf den Kopf stellen. Aber ein kritischer Blick aufs Unternehmen ist dennoch notwendig. Um abschätzen zu können, inwieweit man selbst von der EU-DSGVO betroffen ist, sollte man als Unternehmer bzw Datenschutzbeauftragter einige Fragen für sich beantworten:

1. Wissen Sie, wo und in welcher Form in ihrem Unternehmen überall personenbezogene Daten gespeichert sind?

2. Wie erfolgt(e) die Einwilligung zum Speichern von Daten und ihrer Verwendung? Wie wird bzw wurde diese Einwilligung dokumentiert?

3. Wie wird mit diesen Daten im Unternehmen umgegangen? Welche Prozesse sind für den Datenzugriff, die sichere Speicherung, Backup und Zugriffs-Kontrolle etabliert? Entsprechen diese Tools der EU-DSGVO oder ist es der Initiative der Mitarbeiter überlassen, wie sie zB Kundendaten austauschen und verarbeiten.

4. Gibt es einen Prozess, um Datenabfragen einzelner Personen zu beantworten?

5. Gibt es einen Prozess, zur Löschung personenbezogener Daten auf Wunsch, bzw wenn diese nicht mehr benötigt werden?

6. Welche externen Partner haben Zugriff auf die Daten?

7. Wie wird die Sicherheit personenbezogener Daten gewährleistet?

8. Wie werden alle Prozesse und Datenbewegungen dokumentiert?