ByDe Magazine

DSGVO:
Wer sich nicht vorbereitet, riskiert hohe Bußgelder

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) tritt am 25.05.2018 in Kraft. Umfragen haben ergeben, dass viele Unternehmen noch nicht oder nicht genug mit der Verordnung vertraut sind und nicht den künftigen Anforderungen genügen. Herr Spaeing, warum meinen Sie ist das so?

Thomas Spaeing: Ein wesentlicher Grund ist, dass Datenschutz in vielen Unternehmen immer noch als Randthema wahrgenommen wird, das die eigenen Kernprozesse nicht betrifft. Unternehmen, deren Kernprozess die Verarbeitung personenbezogener Daten ist, sind meist schon ganz anders aufgestellt – allerdings auch nicht alle. Hinzu kommt, dass das Thema Datenschutz komplex ist.

Worin liegen die größten Herausforderungen für Unternehmen bei der Umsetzung der Verordnung?

Die größten Probleme wird die Umstellung der eigenen Prozesse bereiten. Unternehmen müssen die Prozesse ja nicht nur auf dem Papier anpassen, sondern im Tagesgeschäft. Da muss beispielsweise Software angepasst werden, die heute schon nicht optimal gestaltet ist, nach dem 25.05.2018 aber ein echtes Risiko darstellt. Im aktuellen BDSG führen nur wenige Verstöße überhaupt zu einem Bußgeld – und zwar zu einem relativ geringen. Nach der EU-Datenschutz-Grundverordnung sind aber sehr viel mehr Regelungen bußgeldbewehrt und Verstöße werden mit sehr viel höheren Bußgeldern geahndet. So müssen künftig beispielsweise Informations- oder Löschpflichten bereits bei der Entwicklung von Software berücksichtigt werden. Hinzu kommt, dass Dienstleister, die Software oder Cloud-Services anbieten, oft noch nicht bemerkt haben, dass auch sie belangt werden können, wenn ihre Produkte gegen die neue EU-Verordnung verstoßen. Last but not least wird die sogenannte Accountability, also die Nachweispflicht der Rechtmäßigkeit der Datenverarbeitung, vielen Unternehmen nicht möglich sein. Auch hier spielen die Kenntnis der eigenen Prozesse und deren Anpassung an die neuen Anforderungen eine wesentliche Rolle.

Auch wenn es bestimmt schwierig ist, einen Maßnahmenkatalog für unterschiedliche Firmen zu erstellen… Wie sollten Unternehmen vorgehen, um zu erfahren, was sie tun müssen, um die Verordnung künftig zu erfüllen und diese Maßnahmen dann entsprechend umzusetzen?

Der Anpassungsprozess sieht sicher in jedem Unternehmen ein wenig anders aus. Grundsätzlich gibt es aber einige Schritte, die jedes Unternehmen berücksichtigen sollte:

1. GAP-Analyse im Unternehmen: Welche Anforderungen gelten für das Unternehmen und wo steht es hinsichtlich der Erfüllung dieser Anforderungen?
2. Anpassung der Prozesse und Datenverarbeitungen an die neuen Anforderungen

3. Entwicklung der fehlenden Datenschutzprozesse im Unternehmen
4. Schulung der Mitarbeiter zu den neuen Prozessen
5. Definition eines Kontroll- und Verbesserungsprozesses zu den neuen Verfahrens- und Arbeitsanweisungen. Dies leistet beispielsweise ein Datenschutzmanagementsystem. Das kann man durchaus analog zu einem Qualitäts- oder Umweltmanagementsystem sehen – mit dem Unterschied, dass die Norm hier die EU-DSGVO und die weiteren Datenschutzgesetze sind.

Was kann Unternehmen helfen, diese Herausforderung zu meistern – beispielsweise externe Experten, Tools etc.?

„Viele Unternehmen haben das Thema in der Vergangenheit vernachlässigt“

Das hängt davon ab, was bereits vorliegt. Wenn es schon ein Managementsystem in einem anderen Bereich gibt, das gut funktioniert, kann es sinnvoll sein, sich mit den Datenschutzthemen daran zu hängen. Wenn das Unternehmen bereits nach den Regelungen des „alten“ BDSG gut aufgestellt ist, ist der Sprung auch nicht zu groß. Leider haben viele Unternehmen das Thema in der Vergangenheit zu sehr vernachlässigt. Somit gibt es diesbezüglich heute größeren Handlungsbedarf. Tools helfen nur bedingt. Wenn die Expertise im Haus ist, diese mit den richtigen Informationen zu füllen, mag das klappen. Gibt es aber keinen Datenschutzbeauftragten, oder nimmt dieser nur eine Alibifunktion wahr, nützen Tools nichts. Zumal viele auch nicht so sehr prozessorientiert sind, und einen hohen Pflegeaufwand erzeugen. Man muss also genau wissen, was man damit erreichen möchte und wie das geht. Eine Analyse durch einen externen Experten ist sicher hilfreich, da dieser mit einer anderen „Brille“ auf die Themen schaut, als dies interne Prüfer tun. Gibt es eine Audit-Abteilung, so mag auch diese eine einigermaßen neutrale Prüfung hinbekommen, wenn sie das notwendige Know-how besitzt.

Welchen Zeitrahmen brauchen die Unternehmen für diese Vorbereitungen? Wird es knapp bis Mai 2018?

Je nach Komplexität und Umfang der Verarbeitung personenbezogener Daten, kann es bereits zu spät sein. Wenn ein Unternehmen beispielsweise Software von Anbietern aus Drittländern nutzt und diese die neuen Regelungen nicht von sich aus berücksichtigen, kann eine Neuorientierung zu einem EU-Anbieter erforderlich werden. Oder man muss mit dem jetzigen Anbieter über nötige Änderungen verhandeln. Das kostet Zeit und Geld. Viele Unternehmen haben deshalb bereits 2016 Projekte aufgesetzt, um hier rechtzeitig fertig zu werden. Der Termin zum 25.05.2018 steht! Andererseits ist das kein Grund, nichts zu tun. Auch jetzt kann man noch eine Menge erreichen, wenn man keine weitere Zeit mehr verliert und die richtigen Prioritäten setzt. Wenn Schulungen und Kontrollen erst nach dem Stichtag erfolgen, ist das sicher vertretbar. Die Prozesse, beispielsweise zur Wahrung der Rechte der Betroffenen z.B. bei Anfragen oder jene für Datenpannen, sollten dann aber schon stehen. Deutlich mehr Informationen können interessierte Personen beim (BvD) (www.bvdnet.de) erhalten.

Thomas Spaeing, Vorstandsvorsitzender des Berufsverbands der Datenschutz-beauftragten Deutschlands (BvD) e.V. Foto: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.