Kein Grund zur Panik, aber zur Sorgfalt

Illustration: E. Zillner

Am 25. Mai 2018 tritt die neue EU-Datenschutz-Grundverordnung in Kraft. Damit bekommt der Datenschutz einen neuen gewichtigen Stellenwert in den Staaten der Europäischen Union. In dem Gesetz ist die Rede von abschreckenden Strafen, einer umfassenden Dokumentationspflicht, der Auskunftspflicht, der Löschpflicht und der Meldepflicht gegenüber Behörden. Dies gilt für alle Firmen, die personenbezogene Daten besitzen und verarbeiten – auch für kleine und mittlere Betriebe. Sie können nun in Schockstarre verfallen, über die Regelwut des Staates schimpfen, eine teure Beratungsfirma ins Haus holen – oder sich die ganze Sache in aller Ruhe mal etwas genauer ansehen.

Für die meisten deutschen Firmen wird sich nämlich nicht allzu viel ändern. Und was neu hinzukommt, kann mit überschaubarem Aufwand bewältigt werden. Für mittlere und größere Betriebe, in denen mindestens zehn Personen mit der Verwaltung und Bearbeitung personenbezogener Daten zu tun haben, die also Personaldaten pflegen, Kundendaten für die Erstellung von Rechnungen, Gutschriften, Wiege-und Lieferscheinen benutzen oder eine Interessentendatenbank verwalten, besteht ohnehin seit Jahren die Pflicht, einen Datenschutzbeauftragten zu bestellen. Er hat heute schon die Aufgabe die Datenschutzrichtlinien des Betriebes zu dokumentieren, sich von den Fachabteilungen die Beschreibung personenbezogener Verfahren liefern zu lassen, sich als Ansprechpartner zur Verfügung zu stellen und im Bedarfsfall mit der zuständigen Datenschutzbehörde in Kontakt zu treten.

Wirklich neu an der EU-DSGVO ist, dass diese Dokumentations- und Veröffentlichungspflicht ab Mai 2018 auch für kleinere Betriebe gilt. Wichtig ist an dieser Stelle festzuhalten, dass die meisten übrigen Regeln der neuen Grundverordnung auch schon im alten deutschen Datenschutzrecht gegeben waren, und sich die meisten auch kleineren gut organisierten Betriebe im Wesentlichen an diese Vorgaben gehalten haben.

Es ist bei uns einfach üblich, dass Personaldaten entweder vom Chef selber oder wenigen dafür qualifizierten Sachbearbeitern gepflegt und sicher verwahrt werden. Weiter ist es üblich, dass nicht jeder Lehrling oder gewerbliche Mitarbeiter vollen Zugriff auf die kostbaren Kundendaten hat und diese geschützt und gesichert werden. Virenscanner, Firewall und Datensicherheit sind nur noch selten Fremdworte in einem deutschen Betrieb.

Ungewohnt und anfangs lästig ist aber die Dokumentationspflicht des gesamten Umgangs mit dem personenbezogenen Datenmaterial. Für Irritation und Missverständnisse sorgt die fehlende Präzisierung im Gesetz für Klein- und Mittelbetriebe. Dies ist aber dem Umstand geschuldet, das die DSGVO in allen EU-Mitgliedsstaaten gelten wird und zum Beispiel in Deutschland der Datenschutz Ländersache ist, genau gesagt die Aufgabe der Landesdatenschutzbeauftragten und ihrer Behörden. Diese sind ähnlich wie Gerichte unabhängig und nicht an Weisungen ihrer Regierungen gebunden. Es ist nun Sache dieser Landesämter, die Richtlinien für ihren Zuständigkeitsbereich zu benennen und bekannt zu machen. Eine besondere Stellung bei diesen Behörden nimmt das Bayerische Landesamt für Datenschutzaufsicht in Ansbach ein. Das liegt vor allem an dessen Chef Thomas Kranig. Kranig ist einer der profiliertesten und kompetentesten deutschen Datenschutzfachleute. Was Kranig sagt, gilt.

Kranig und seine Behörde haben dankenswerter Weise 2017 mit dem C. H. Beck

Foto: Martina Leiacker

Von Klaus Rederer

Dr. Klaus Rederer ist EDV-Sachverständiger, Datenschutzauditor und Geschäftsführer der rekom GmbH, die seit dem Jahr 2000 mit EUREC - Die Recyclingsoftware im deutschen Schrotthandel bekannt ist.

Verlag in München ein „Sofortmaßnahmen-Paket“ zur DSGVO herausgegeben. Die 60-seitige Schrift trägt den Namen: „Erste Hilfe zur Datenschutz Grundverordnung für Unternehmen und Vereine“. Hier findet man anschaulich, nachvollziehbar und sehr pragmatisch dargestellt, was nun wirklich zu tun ist. Es wird aber auch mehrfach darauf hingewiesen, dass harte Sanktionen drohen, wenn ein Betrieb diese Vorgaben ignoriert. Kranigs Grundhaltung ist: Tun Sie das Nötige, bevor es zu spät ist.

Das Wichtigste hier ist die Dokumentation, also die Erarbeitung einer eigenen betrieblichen Datenschutzrichtlinie. In dieser Richtlinie, die der Firmengröße und dem Umfang der Verarbeitung personenbezogener Daten angemessen sein soll; im kleinen Betrieb knapp, präzise und unter Berücksichtigung nur weniger formaler Vorgaben. Hier sind ausdrücklich nicht die umfangreichen und entsprechend aufwändigen umzusetzenden Vorgaben der ISO Normen ISO 27001 oder ISO 9001 gemeint, aber sehr wohl deren Kern.

- So ist als erstes klarzustellen und festzuhalten, wer für welche Aufgaben zuständig ist, im Zweifelsfall immer der Chef und er ist dann auch nach außen als Verantwortlicher zu benennen.
- Es ist eine Bestandsaufnahme aller Verfahren durchzuführen und zu dokumentieren, in denen personenbezogene Daten verarbeitet werden.
- Es ist ein Verzeichnis dieser Verarbeitungstätigkeiten zu erstellen; praktisch heißt das z. B. eine kurze Beschreibung des Personalwesens, mit Benennung der Zuständigkeiten und Sicherheitsvorkehrungen, oder eine knappe Beschreibung der Vorgänge zur Erstellung von Rechnungen, Gutschriften, Lieferscheinen, Containeraufträgen und Verwiegungen, in denen Personen- und Adressdaten verarbeitet werden.
- Für diese Abläufe sind die Rechtsgrundlagen zu benennen, z.B. Artikel 6 DSVGO „Rechtmäßigkeit der Verarbeitung“ …
- … und nötigenfalls wirksame Einwilligungserklärungen der Betroffenen zu formulieren, dokumentieren und einzuholen.
- Weiter ist zu klären, ob die Dienste sogenannter Auftragsverarbeiter in Anspruch genommen werden und die hierfür erforderlichen Verträge abgeschlossen sind; typische Auftragsverarbeiter sind EDV-Systembetreuer oder Softwarehersteller, mit denen Sie einen Supportvertrag haben. Zuständig für die Formulierung und den Abschluss dieser Verträge ist immer der Auftraggeber.
- Zu klären ist, ob die Rechte der Betroffenen eingehalten werden, deren Daten Sie besitzen und verarbeiten. Das sind im Wesentlichen die Informationspflicht, das Auskunftsrecht, das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Datenübertragbarkeit, das Widerspruchsrecht. Stellen Sie zudem sicher, dass Sie in diesen Fällen Ihren Verpflichtungen in angemessener Zeit nachkommen können und dokumentieren Sie dies.
- Erarbeiten Sie eine eigene Datenschutzerklärung und veröffentlichen Sie diese in Ihrem betrieblichen Aushang und auf Ihrer Homepage.
- Dokumentieren Sie, wie Sie mit einer erkannten meldepflichtigen Datenschutzverletzung umgehen.
- Halten Sie fest, welche Maßnahmen Sie in der Datensicherung und -sicherheit ergriffen haben und ob die von Ihnen verwendete (EDV-)Technik in ihrer Gestaltung über datenschutzfreundliche Voreinstellungen verfügt; verantwortlich sind Sie, nicht der Hersteller oder Lieferant von Hardware und Software.
- Beschreiben Sie, wie Sie Änderungen Ihrer betrieblichen Verfahren dokumentieren, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben.
- Stellen Sie sicher und weisen nach, wann und wie Sie Ihre Mitarbeiterinnen und Mitarbeiter in regelmäßigen Abständen bezüglich der Einhaltung des Datenschutzes, sensibilisieren, selbst schulen oder qualifizieren lassen.

Die Erstellung einer solchen Datenschutzrichtlinie dient auch als Leitfaden für die spätere Umsetzung und wird ab Mai 2018 bei einer Überprüfung oder im Falle einer Kontrolle aufgrund eines Verstoßes als erstes überprüft. Fehlt eine brauchbare Dokumentation der Datenschutzmaßnahmen, ist allein dies aufgrund der gesetzlichen Vorgaben Grund für eine empfindliche Geldstrafe. Verfügen Sie jedoch über eine gut gemachte und aktuell gehaltene Datenschutzrichtlinie, deren Einhaltung im Optimalfall von einem Auditor überprüft wurde, sind Sie auf der sicheren Seite und kommen wahrscheinlich im Fall eines minder schweren Verstoßes mit einem blauen Auge davon.

In der Recyclingbranche, die seit Jahren gewohnt ist, die Vorgaben der Finanzämter, des Umwelt- und Abfallrechts einzuhalten, in der Betriebstagebücher, Abfallregister und entsprechende Zertifizierungsverfahren gang und gäbe sind, dürfte auch die Umsetzung dieses Katalogs eine machbare Herausforderung sein.

In Kranigs Sofortmaßnahmenpaket werden brauchbare Handlungsanweisungen gegeben, an guten Beispielen mögliche Formulierungen benannt und nahezu alle notwendigen Formulare und Muster geliefert. Die sonst derzeit auf dem Markt verfügbare Literatur zum Thema ist meist nicht geeignet, weil sie sich zu stark an den Notwendigkeiten größerer Betriebe mit wesentlich komplexeren Abläufen orientiert. Das Gesetz selbst ist erstaunlich gut lesbar geschrieben, so dass es meist sinnvoll ist, diesen Text direkt zu konsultieren, als sich in einer nicht wirklich passenden Sekundärliteratur zu verirren.

Sollten Sie sich entscheiden, bei der Bewältigung der hier anstehenden Aufgabe externen Sachverstand heran zu ziehen, achten Sie unbedingt darauf, dass infrage kommende Anwaltskanzleien oder externe Datenschutzbeauftragte ein Konzept auch für kleine Betriebe haben. Das ist heute oft noch ein Problem, weil vor allem die Dokumentation der Datenschutzbemühungen im kleineren Betrieb bisher nur in seltenen Fällen ins Arbeitsgebiet von Rechtsanwälten oder professionellen Datenschützern fiel. Dasselbe gilt für die fachlich oft sehr guten Seminare von Anbietern wie dem TÜV, der DEKRA oder Modal. Diese gehen oft über mehrere Tage und richten sich im Schwerpunkt an hochqualifizierte Fachleute und deren spezielle Befindlichkeiten. *Dr. Klaus Rederer, Rekom*