

Recht: Datenschutz – jetzt wird's ernst



AUS DEN VERBÄNDEN



Bislang war der Datenschutz in Deutschland weitgehend im Bundesdatenschutzgesetz (BDSG) geregelt. Dies Gesetz ist klar und einigermaßen streng, aber bei genauer Betrachtung nur für inländische Betriebe ab einer gewissen Größenordnung relevant.

Dennoch bislang gilt: Haben in einer Firma weniger als zehn Mitarbeiter mit den sogenannten personenbezogenen Daten (Namen, Adressen, Telefonnummern usw.) zu tun, muss kein Datenschutzbeauftragter bestellt werden, und wenn keine größeren Verstöße bekannt werden, gibt es kaum jemanden, der nach Einhaltung der gegebenen Regeln fragt. Die zuständigen Landesdatenschutzbehörden sind personell sehr bescheiden ausgestattet und verhängen, wenn überhaupt, harmlose Bußgelder.

Aber am 25. Mai 2018 ändert sich das grundlegend, dann 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. Einen besonderen Stellenwert nimmt hier die unmissverständliche Verpflichtung ein, dass sämtliche Prozesse, die mit personenbezogenen



Foto: Rederer

Dr. Klaus Rederer:

„Das Wichtigste ist die Dokumentation, also die Erarbeitung einer eigenen betrieblichen Datenschutzrichtlinie.“

Daten zu tun haben, definiert und schriftlich in einem sogenannten Verfahrensverzeichnis festgehalten werden. Es genügt also zukünftig nicht mehr, mit diesen Daten sorgfältig und gewissenhaft umzugehen, die Gesetze zu befolgen und keinen Missbrauch zu treiben. Dies muss nun zwingend dokumentiert werden. Wie macht man das? Worauf kommt es an?

Genau das ist für Ungeübte nicht einfach zu erkennen, für Irritation und Missverständnisse sorgt zunächst die fehlende Präzisierung im Gesetz für Klein- und Mittelbetriebe. Dies ist aber dem Umstand geschuldet, dass die DSGVO in allen EU-Mitgliedstaaten gelten wird und z. B. in Deutschland der Datenschutz Ländersache ist, genauer gesagt die Aufgabe der Landesdatenschutzbeauftragten und ihrer Behörden. Diese Behörden haben sich aber bisher weitgehend vornehm zurückgehalten, klar nachvollziehbare rechtlich verbindliche Richtlinien zu entwickeln und zu veröffentlichen. Eine rühmliche Ausnahme macht hier Thomas Kranig, der Chef des Bayerischen Landesamts für Datenschutzaufsicht in Ansbach. Zwar veröffentlicht auch seine Dienststelle ihre Erkenntnisse nicht selbst und umfassend, aber Kranig hat mit dem C. H.

Beck 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.

Das Wichtigste ist die Dokumentation, also die Erarbeitung einer eigenen betrieblichen Datenschutzrichtlinie. Diese soll der Firmengröße und dem Umfang der Verarbeitung personenbezogener Daten angemessen sein; im kleinen Betrieb knapp, präzise und unter Berücksichtigung nur weniger formaler Vorgaben. Hier sind ausdrücklich nicht die umfangreichen und entsprechend aufwendigen 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 DSGVO „Rechtmäßigkeit der Verarbeitung“ ...
- ... und nötigenfalls wirksame Einwilligungserklärungen der Betroffenen zu formulieren, dokumentieren und einzuholen.
- Zu klären ist, ob die Rechte der Betroffenen, also der Personen 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.
- 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.
- 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.

Im Sofortmaßnahmenpaket des C. H. Beck Verlags werden brauchbare Handlungsanweisungen gegeben, an guten Beispielen mögliche Formulierungen vorgeschlagen und nahezu alle notwendigen Formulare und Muster geliefert. Die sonst derzeit auf dem Markt verfügbare Literatur zum Thema ist dagegen 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, sodass es meist mehr Sinn macht, diesen Text direkt zu konsultieren, als sich in einer nicht wirklich passenden Sekundärliteratur zu verirren. Die fachlich oft sehr guten Seminare von Anbietern wie dem TÜV, der DEKRA oder Modal gehen oft über mehrere Tage und richten sich im Schwerpunkt an hochqualifizierte Fachleute und deren Befindlichkeiten. Spezielle Angebote für kleinere Unternehmen und deren Bedürfnisse sind meist noch in der Entwicklung, kommen aber nach und nach auf den Markt. So bietet z. B. die Firma arborsys ab April 2018 einen halbtägigen Workshop zur Selbsthilfe an.

Sollten Sie sich entscheiden, bei der Bewältigung der hier anstehenden Aufgabe externen Sachverstand heranzuziehen, achten Sie unbedingt darauf, dass infrage kommende Anwaltskanzleien oder externe Datenschutzbeauftragte, die in diesem Feld ihre Dienste anbieten, 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.

(Ein Beitrag von Dr. Klaus Rederer, Datenschutz-Sachverständiger (DESAG) und Geschäftsführer der rekom GmbH)

klaus.rederer@rekom.de

recycling
aktiv

Stein-Verlag Baden-Baden GmbH
Josef-Herrmann-Straße 1–3
D-76473 Iffezheim
Tel.: +49 7229 606-0
Fax: +49 7229 606-10
infoSTV@stein-verlagGmbH.de
www.stein-verlagGmbH.de