Datenschutz im Unternehmen:

Neue Grundverordnung zwingt zum Handeln

„EU-Datenschutz-Grundverordnung“ – das klingt nach Bürokratie pur. Nach etwas, womit man sich nicht auseinandersetzt, wenn es nicht sein muss. Das Problem: Es muss sein, es ist fünf vor zwölf für Unternehmen, die ihre Prozesse und Verfahren noch nicht an die „EU DS-GVO“ angepasst haben. Denn sie tritt am 25.5.2018 in Kraft und wird die nationalen Datenschutzgesetze EU-weit weitestgehend ablösen – mit erheblichen Konsequenzen für Betriebe.

Die DS-GVO entfaltet unmittelbare Wirkung in jedem Mitgliedstaat der Europäischen Union. Ihr Gesetzestext muss nicht erst in nationales Recht umgesetzt werden, sondern kommt direkt zur Anwendung. Allerdings werden den nationalen Gesetzgebern zu regelnde Pflichtbestandteile auferlegt, aber auch Öffnungsklauseln ermöglicht, die den Mitgliedstaaten spezielle Gestaltungsspielräume eröffnen. Diese Sachverhalte werden in Deutschland durch das bereits beschlossene „Bundesdatenschutzgesetz 2018“ – kurz: BDSG-neu – geregelt. Die Änderungen im Bundesdatenschutzgesetz werden gemeinsam mit der DS-GVO am 25.5.2018 in Kraft treten.

Was bedeutet das für Unternehmen? Einfach gesprochen: einen neuen und in Teilen schärferen Rahmen für den Datenschutz. Dabei spielt es keine Rolle, in welcher Branche ein Betrieb tätig ist oder wie groß er ist. Sobald regelmäßig personenbezogene Daten verarbeitet werden, sind die Vorgaben des neuen Rechts bindend – ohne Wenn und Aber. Als personenbezogene Daten gelten hier alle Angaben über identifizierte oder identifizierbare natürliche Person. Dazu gehören beispielsweise Namen, Kontaktdaten oder Bankverbindungen.

Allgemeine Grundsätze: wichtig für die Auslegung

Art. 5 Abs. 1 der DS-GVO enthält die sogenannten allgemeinen Datenschutzgrundsätze. Sie sind wichtig für die Auslegung der gesetzlichen Regelungen. Hier werden grundlegende Themen der Datenverarbeitung abgehandelt: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz und Zweckbindung ebenso wie Datenminimierung, Richtigkeit, Begrenzung der Speicherdauer und Integrität sowie Vertraulichkeit. Art. 5 Abs. 2 führt im Folgenden einen Begriff ein, den das deutsche Daten-

schutzrecht so bislang nicht verwendete: die Rechenschaftspflicht. Diese Änderung ist elementar. Sie bedeutet: Die Verantwortlichen in Unternehmen sind nicht nur zur Einhaltung der im neuen Gesetz normierten Prinzipien verpflichtet. Sie müssen auch nachweisen können, dass sie diese einhalten.

Datenverarbeitung: nicht ohne gesetzliche Grundlagen

Eine Datenverarbeitung ist nur zulässig, wenn es die Verordnung oder ein anderes Gesetz ausdrücklich erlaubt. Man spricht in diesem Zusammenhang von einem „Verbot mit Erlaubnisvorbehalt". Ansonsten ist sie nur mit Einwilligung des Betroffenen möglich. Art. 7 DS-GVO legt fest: Eine Einwilligung gilt nur dann als wirksam erteilt, wenn der Betroffene in Kenntnis des Umfangs der geplanten Verarbeitung sowie freiwillig und unmissverständlich sein Einverständnis für den konkreten Fall der Verarbeitung erteilt. Bereits bei Erteilung der Einwilligung muss der Betroffene zudem auf sein Widerrufsrecht hingewiesen werden. Deshalb sollten datenverarbeitende Unternehmen im eigenen Interesse schnellstmöglich ihre bisherigen Einwilligungserklärungen auf Konformität mit der DS-GVO prüfen und die Erklärungen gegebenenfalls anpassen, vor allem aus Nachweisgründen.

Fast jedes Unternehmen verarbeitet Daten

Wichtig ist außerdem, sich klarzumachen, um wessen Rechte es geht. Mit Sicherheit denkt jeder zunächst an Kundendaten. Doch auch die zu Mitarbeitern, Bewerbern, Interessenten oder Lieferanten gesammelten Daten sind grundsätzlich nachweisbar zu schützen. Aus diesem Grund sollten Verantwortliche in Unternehmen sich Klarheit über die genauen Rechte dieser Gruppen verschaffen – insbesondere über ihre Informations-, Auskunfts- und Widerspruchsrechte sowie das Recht auf Berichtigung, Löschung und Einschränkung („Sperrung").

Neu ist das Recht des Betroffenen auf Datenübertragbarkeit: Wenn etwa ein Nutzer eines sozialen Netzwerks oder eines Cloud-Anbieters in ein anderes Social Network oder zu einem anderen Cloud-Provider wechselt, hat er unter bestimmten Voraussetzungen das Recht, seine gespeicherten personenbezogenen Daten in einem geeigneten Format zu erhalten (zum Beispiel auf einem USB-Stick oder per verschlüsselter E-Mail), um diese an den neuen Anbieter zu übermitteln oder von Anbieter zu Anbieter übermitteln zu lassen.

Ein Verzeichnis muss her

Ein wesentliches Instrument der DS-GVO ist das „Verzeichnis der Verarbeitungstätigkeiten" (Art. 30 DS-GVO, bisher „Verfahrensverzeichnis"). Es ist ein zentraler Bestandteil der Datenschutzdokumentation und listet alle Verfahren auf, die personenbezogene Daten verarbeiten – so etwa Buchhaltungssysteme, Personaldatenverwaltung oder Videoüberwachung. Auch enthält das Verzeichnis Informationen wie etwa den Zweck der Verarbeitung, Datenkategorien, Empfänger, Löschfristen und technische sowie organisatorische Schutzmaßnahmen. Bei jeder Verarbeitung ist eine Risikobewertung bezüglich der Rechte und Freiheiten natürlicher Personen durchzuführen und zu dokumentieren.

Maßnahmen zur Datensicherheit ergreifen

Verantwortliche müssen geeignete technische und organisatorische Maßnahmen (TOM, Art. 32 DS-GVO) treffen, um die Datensicherheit zu gewährleisten. Welche Maßnahmen konkret erforderlich sind, hängt unter anderem vom Stand der Technik, dem Verarbeitungsumfang und -zweck sowie

AUTOR

***Dipl.-Ökonom Bernd Schulz** ist Unternehmensberater u.a. mit dem Schwerpunkt betriebliches Risikomanagement sowie vom TÜV zertifizierter (externer) Datenschutzbeauftragter. In dieser Funktion ist er für mehrere mittelständische Unternehmen im Ruhrgebiet bzw. Münsterland tätig. Er studierte Wirtschaftswissenschaften an der Ruhr-Universität Bochum und ist seit 2003 bdvb-Mitglied.*
http://datenschutz.bcschulz.de/

von der Risikoeinschätzung ab. Als Schutzmaßnahmen führt die DS-GVO explizit die Pseudonymisierung und Verschlüsselung personenbezogener Daten auf.

Führt die Risikoanalyse zu dem Ergebnis, dass die Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bedeutet, ist eine Datenschutz-Folgenabschätzung (Art. 35 DS-GVO, bisher „Vorabkontrolle") durchzuführen. Sie ist mit einer umfassenden Dokumentation verbunden – unter anderem mit einer systematischen Beschreibung der Verarbeitungsvorgänge und -zwecke, möglicher Risiken für die Betroffenen sowie getroffener bzw. geplanter Schutzmaßnahmen. Kommt die Bewertung zu dem Ergebnis, dass trotz möglicher Maßnahmen ein Restrisiko besteht, muss in einer weiteren Stufe die Aufsichtsbehörde konsultiert werden.

Auftragsverarbeitung: bestehende Verträge anpassen

Werden personenbezogenen Daten durch einen Dienstleister erhoben, verarbeitet oder genutzt – beispielsweise beim Einsatz von Call-Centern – handelt es sich um eine Auftragsverarbeitung (bisher „Auftragsdatenverarbeitung"). Hier definiert Art. 28 DS-GVO eine Vielzahl von Vorgaben für die Vertragsgestaltung. Bestehende Verträge sollten in solchen Fällen an die Grundverordnung angepasst werden. Denkbar ist beispielsweise der Abschluss einer neuen Vereinbarung oder die Unterzeichnung einer Zusatzvereinbarung, die alle neuen Regelungstatbestände berücksichtigt.

Haftungsrisiko wächst

Fehler während der Datenverarbeitung können Betroffenen erheblichen Schaden zufügen. Sie sollen Haftungsansprüche künftig leichter geltend machen können. Unternehmen sind damit einem deutlich höheren Haftungsrisiko ausgesetzt, der Rahmen für Bußgelder wird drastisch erhöht. Künftig betragen die Obergrenzen je nach Verstoß 10 Millionen Euro bzw. 20 Millionen Euro (Art. 83 DS-GVO). Im Falle einer Verletzung des Schutzes personenbezogener Daten ist zudem bei Vorliegen bestimmter Voraussetzungen binnen 72 Stunden eine unverzügliche Meldung an die Aufsichtsbehörde erforderlich. Unter Umständen sind die Betroffenen ebenso zu informieren.

Ein wichtiger Aspekt ist in diesem Zusammenhang die Beweislastumkehr: Derzeit stehen die Betroffenen in der Nachweispflicht, dass ein Unternehmen oder eine Behörde für Schäden aus fehlerhafter Datenverarbeitung haftbar ist. Künftig muss die datenverarbeitende Stelle nachweisen und anhand von Dokumenten belegen können, dass sie rechtskonform arbeitet.

Mehr Datenschutzbeauftragte im Land

Nach Art. 37 DS-GVO müssen Unternehmen immer dann einen betrieblichen Datenschutzbeauftragten benennen, wenn ihre Kerntätigkeit in umfangreicher oder systematischer Überwachung von Personen oder der umfangreichen Verarbeitung besonderer Datenkategorien wie etwa Gesundheitsdaten besteht.

Das BDSG-neu erweitert die Gründe für die Benennung eines Datenschutzbeauftragten. Sie ist danach wie bisher auch dann erforderlich, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Datenverarbeitung beschäftigt sind. Unabhängig von der Personenanzahl ist ein Datenschutzbeauftragter zu benennen, wenn Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Erste Schritte

Fünf vor zwölf heißt: Es ist Zeit zu handeln. Doch wo fängt man am besten an, um sich möglichst rechtzeitig rechtssicher aufzustellen? Folgende Maßnahmen dürfen als „Wegweiser" durch die erforderlichen Umstellungsprozesse gelten:

- Geschäftsleitung und Entscheidungsträger für die Anforderungen der DS-GVO sensibilisieren
- Internen oder externen Datenschutzbeauftragten einbinden
- Rechtliche und organisatorische Rahmenbedingungen der Prozesse zur Datenverarbeitung (Ist-Zustand) analysieren
- Soll-Zustand definieren und Lückenanalyse zum Ist-Zustand aufstellen – etwa anhand der oben genannten Bestandteile der DS-GVO
- Verfahren und Strukturen unter Beachtung von Rechtsgrundlagen, Verarbeitungszwecken und Betroffenenrechten angleichen
- Datenschutzorganisation hinsichtlich Nachweis- und Dokumentationspflichten, Vertrags- und Einwilligungsmanagement sowie Reaktionsmechanismen auf Datenpannen anpassen
- Mitarbeiterinnen und Mitarbeiter zu Anforderungen der DS-GVO schulen «