Industrie- und Handelskammer
Osnabrück - Emsland - Grafschaft Bentheim

Stichtag 25. Mai 2018: EU-Datenschutzrecht

Am 25. Mai 2018 wird das deutsche Datenschutzrecht durch die Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO) ersetzt. Immense Bußgelddrohungen sind die plakativste Veränderung. Was müssen unsere Unternehmen jetzt tun? Wir geben ihnen einen Überblick über die Änderungen und Tipps zur Vorbereitung auf das neue Recht.

Was für Daten schützt das Datenschutzrecht?

Das Datenschutzrecht schützt personenbezogene Daten, d. h. Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Dazu gehören nicht nur Name, Geburtsdatum etc. sondern auch alle sonstigen Informationen von der IP-Adresse über die Kundenhistorie bis zu Gewohnheiten. Geschützt werden also in allen Unternehmen Kunden- und Lieferantendaten genauso wie Mitarbeiterdaten.

Jedes Unternehmen ist betroffen

Zur Einhaltung und Dokumentation des Datenschutzes verpflichtet sind alle Unternehmen und Behörden, die personenbezogene Daten verarbeiten – also alle, selbst Ein-Personen-Unternehmen.
Zwar müssen kleine Unternehmen, die keine sensiblen Daten verarbeiten, keinen Datenschutzbeauftragten bestellen. Alle anderen Regeln gelten für sie aber trotzdem.

EU-DSGVO + BDSG-neu ersetzen altes BDSG

Das neue Datenschutzrecht hat die EU als Verordnung geregelt. Das bedeutet, dass es unmittelbar in allen Mitgliedstaaten gilt. Das neue BDSG tritt am selben Tag in Kraft und ergänzt die EU-Regeln überall dort, wo die DSGVO sog. Öffnungsklauseln enthält.
Ein gutes Beispiel dafür sind die Regelungen zum Datenschutzbeauftragten: Art. 37 DSGVO regelt zunächst die Stellung des Datenschutzbeauftragten sowie die Pflicht, einen zu bestellen, für Behörden und für Unternehmen, die besonders sensible Daten verarbeiten, z. B. Auskunfteien und Gesundheitseinrichtungen. Darüber hinaus erlaubt er den Mitgliedstaaten, weitere Bestellungspflichten festzulegen. Das nutzt das BDSG-neu, indem es in § 38 die bisherige Regelung, dass ein Datenschutzbeauftragter u. a. zu bestellen ist, wenn mindestens zehn Personen ständig mit der automatisierten Datenverarbeitung beschäftigt sind, erneut festschreibt.

Bewährte Grundregeln

Nicht nur beim Datenschutzbeauftragten verändert sich wenig. Auch die sonstigen Prinzipien des deutschen Datenschutzrechts bleiben erhalten: Verbot mit Erlaubnisvorbehalt sowie Datensparsamkeit und Datensicherheit

Grundsatz des Datenschutzrechts ist das Verbot mit Erlaubnisvorbehalt, dass personenbezogene Daten nur erheben und verarbeiten darf, wer dafür eine Legitimation hat. Das kann eine Erlaubnisvorschrift im Gesetz oder eine Einwilligung des Betroffenen sein. Erlaubt ist z. B. die Verarbeitung aller Daten, die man für die Abwicklung eines konkreten Vertragsverhältnisses braucht.

Bei der Verarbeitung stehen dann Datensparsamkeit und Datensicherheit im Vordergrund. Datensparsamkeit verlangt als Erstes, jede Datenverarbeitung darauf zu prüfen, welche personenbezogenen Daten wirklich und wie lange für den jeweiligen Zweck erforderlich sind, ob ggf. auch eine Pseudonymisierung oder Anonymisierung möglich ist. Datensicherheit erfordert ein umfassendes Konzept aus technischen und organisatorischen Maßnahmen, damit die legal erhobenen Daten weder verfälscht noch missbraucht werden können.

Rechenschaftsprinzip: umfangreiche Dokumentation

Neu ist dagegen das Rechenschaftsprinzip: Der/die Verantwortliche, also die Unternehmensleitung, muss durch eine umfangreiche Dokumentation nachweisen, dass die Datenschutzregeln eingehalten werden. Das reicht vom Verzeichnis von Verarbeitungstätigkeiten (bisher: Verfahrensverzeichnis) bis zu Checklisten für eventuelle Datenschutzpannen.

Informations- und Auskunftspflichten

Ein typisches Beispiel für die Rechenschaftspflichten bietet der Anspruch Betroffener auf Auskunft über alle über sie gespeicherten Daten. Auch das alte BDSG enthält diesen Anspruch. Die DSGVO verlangt aber über die individuelle Auskunft hinaus, dass jedes Unternehmen einen Ablaufplan o. Ä. vorhält, der sicherstellt, dass dann, falls wirklich einmal dieser Auskunftsanspruch geltend gemacht wird, die Auskunft auch tatsächlich umfassend und fristgerecht erteilt werden kann. Außerdem erweitert die DSGVO die Informationspflichten gegenüber Betroffenen über die Verarbeitung ihrer Daten.

Einwilligung

Wenn eine Datenverarbeitung nur mit Einwilligung erlaubt ist, muss diese Einwilligung auch den Vorgaben entsprechen. D. h. sie muss freiwillig und ausdrücklich erfolgen. Dazu muss der Zweck der Datenverarbeitung konkret genug beschrieben werden. Die DSGVO schreibt zwar keine Schriftform vor, doch muss der Unternehmer die Einwilligung im Zweifelsfall ja nachweisen können. Insofern ist sie schriftlich, im Internet per „Double Opt In“ oder telefonisch per Tonaufzeichnung abzusichern. Einwilligungen müssen jederzeit widerruflich sein – und auf die Widerrufsmöglichkeit ist natürlich ausdrücklich hinzuweisen.

Datenschutzfolgenabschätzung

Die DSGVO arbeitet verstärkt mit dem risikobasierten Ansatz, wie er vielen aus dem Qualitätsmanagement vertraut ist. Daraus folgt zum Beispiel, dass bei jeder geplanten Verarbeitung personenbezogener Daten, die gewisse Risiken enthält, zunächst abgeschätzt werden muss, welche Risiken für die Betroffenen entstehen, wie schwer sie sind und wie hoch die Eintrittswahrscheinlichkeit ist. Daraus müssen dann Maßnahmen technischer und organisatorischer Art abgeleitet werden, mit denen die Risiken verringert werden. Die Datenschutzfolgeabschätzung ist die Weiterentwicklung der bisherigen Vorabkontrolle, wie sie z. B. für Videoüberwachungen schon jetzt zwingend ist.

Schärfere Sanktionen

Je nachdem, gegen welche Norm der DSGVO verstoßen wird, muss mit Bußgeldern von bis zu zehn Millionen Euro bzw. zwei Prozent des weltweiten Vorjahresumsatzes, in bestimmten Fällen bis zu 20 Millionen Euro bzw. vier Prozent des weltweiten Jahresumsatzes gerechnet werden. Bislang liegt das Maximum bei 300.000 Euro.

Zuständig für Bußgelder und Strafen sind die Datenschutzbeauftragten der Bundesländer. Die Niedersächsische Landesdatenschutzbeauftragte selbst sieht ihre Funktion mindestens ebenso in der Beratung wie in der Kontrolle. Systematische Kontrollen fanden bisher bei bestimmten Branchen, z. B. Auskunfteien oder Call Centern, oder zu bestimmten Themen, z. B. Datenübermittlung in Drittstaaten, statt. Auch unter der DSGVO dürfte es so bleiben, dass einzelne kleine Unternehmen ohne besonders sensible Datenströme eher aus konkretem Anlass in den Fokus der Aufsicht geraten. Die größten Risiken können dabei nicht einmal von unzufriedenen Kunden, sondern vor allem von im Streit ausgeschiedenen Mitarbeitern ausgehen. Wenn diese die Schwachstellen im Datenschutz ihres ehemaligen Arbeitgebers kennen, können sie ihm durch eine gezielte Anzeige viel Arbeit mit der Datenschutzaufsicht verschaffen.

Wo fange ich an?

Wenn ein Unternehmen sich bisher noch gar nicht oder kaum um den Datenschutz gekümmert hat, ist es höchste Zeit, damit anzufangen. Jeder Schritt, der erledigt ist, verringert die Gefahr eines Bußgelds.

- Als erstes sollte geprüft werden, ob ein Datenschutzbeauftragter bestellt werden muss.
- Parallel sollte mit dem Aufbau des Verzeichnisses der Verarbeitungstätigkeiten begonnen werden: Alle Prozesse im Unternehmen, bei denen Kunden-, Lieferanten- oder Mitarbeiterdaten verarbeitet werden, werden aufgelistet. Dann wird für jeden dieser Prozesse eine kurze Verfahrensbeschreibung erstellt. Beim Ausfüllen stellen sich die Standardfragen für jeden dieser Prozesse: Ist die Verarbeitung all dieser Daten für den konkreten Zweck notwendig? Ist der Kreis der Zugriffsberechtigten bereits technisch so klein wie möglich? Wann können die Daten gelöscht werden?
- Die eigenen Antworten sollten genutzt werden, um die Verarbeitungsprozesse zu optimieren.
- Auch können die jeweiligen Vereinbarungen zur Auftragsdatenverarbeitung den einzelnen Verarbeitungstätigkeiten zugeordnet werden.“
- Nächster Schritt ist die Zusammenstellung aller technischen und organisatorischen Maßnahmen zur Datensicherheit, die das Unternehmen nutzt, z. B. Türschlösser, Berechtigungskonzept und Passwortschutz, Firewall und Sicherungskopien von Festplatten genauso wie die Dienstanweisungen und Betriebsvereinbarungen zur E-Mail-Nutzung, zur Passwortbildung- und Geheimhaltung, die Verpflichtung aller Mitarbeiter auf das Datengeheimnis etc.
- Nun folgen die Handlungsanweisungen zum Vorgehen bei Datenschutzverstößen, Datenübertragungen und Auskunftsverlangen Betroffener.
- Ausformulierte Datenschutzrichtlinien zur Verarbeitung von Arbeitnehmerdaten sowie zu Kundendaten runden das Datenschutzmanagement ab.
- Ferner ist auch die Datenschutzerklärung zu aktualisieren bzw zu erstellen, in der Personen, die mit dem Unternehmen in Kontakt treten, über die Nutzung ihrer personenbezogenen Daten informiert werden.

Mitarbeiterschulung

Last but not least nutzt das beste Datenschutzkonzept natürlich nichts, wenn die Mitarbeiter es im Alltag nicht umsetzen. Deswegen ist ein wichtiger Baustein im Datenschutzmanagement die regelmäßige Schulung und Sensibilisierung der Mitarbeiter.

Hilfestellung

Wer professionelle Hilfe im Datenschutzbereich sucht, kann z. B. einen externen Dienstleister damit betrauen. Dabei gibt es sowohl die Möglichkeit, den Externen direkt zum Datenschutzbeauftragten zu ernennen, so dass er das Unternehmen dauerhaft im Datenschutz betreut, oder seine Beratungsleistung nur anlassbezogen einzukaufen, typischerweise als Unterstützung für den internen Datenschutzbeauftragten bei besonderen Herausforderungen wie z. B. dem erstmaligen Aufbau des Datenschutzmanagements.

Kleine Betriebe, die keinen Datenschutzbeauftragten brauchen und aus Kostengründen auf externe Beratung verzichten, finden im Internet diverse Hilfestellungen. Vor allem die Niedersächsische Landesdatenschutzbeauftragte veröffentlicht inzwischen auf ihrer Homepage www.lfd.niedersachsen.de einen Katalog von Fragen zur Vorbereitung auf die DSGVO sowie laufend neue Kurzpapiere, die praktische Hinweise zu den einzelnen Themen geben sollen, aber auch z. B. ein Muster für das Verzeichnis der Verarbeitungstätigkeiten, Formulierungshilfen für die Auftragsdatenverarbeitungsvereinbarung sowie Vorlagen für die Beschilderung von Videoüberwachung. Vorteil dieser Hilfen ist, dass sie direkt von der Aufsichtsbehörde kommen, ihre Umsetzung also stark entlastende Wirkung haben dürfte, wenn es tatsächlich zu einem Verfahren kommen sollte.

Auch auf der Seite der IHK www.osnabrueck.ihk.de finden sich unter der Dok.-Nr. 3757926 laufend ergänzte Merkblätter zur DSGVO sowie ein Muster für das Verzeichnis der Verarbeitungstätigkeiten.

Mit diesen Mitteln und etwas Zeit kann jede Unternehmerin und jeder Unternehmer ein Grundgerüst an Datenschutzmaßnahmen für ihren/seinen Betrieb errichten und damit das Risiko eines Bußgeldes erheblich reduzieren.