

Datenschutzverordnung tritt zum 25. Mai in Kraft

Die DSGVO enthält einige Neuerungen. So ist etwa der Verlust oder Missbrauch von Daten binnen 72 Stunden nach Kenntnis an die Landes- Aufsichtsbehörde für Datenschutz und Informationsfreiheit zu melden. Fest steht: Sind die persönlichen Rechte der Betroffenen nicht verletzt, entfällt die Meldepflicht.

Hohe Strafen

Was außerdem einen vermehrten Aufwand darstellt: Jede Datenschutzverletzung ist zu dokumentieren. Und: Datenschutzverletzungen sollten nicht auf die leichte Schulter genommen werden. Denn die Bußgelder sind enorm. Bei einem Verstoß stehen Strafen von bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Gesamtumsatzes im Raum. Für manche Unternehmen kann dies die Existenz gefährden. Doch greifen diese hohen Strafen erst in besonders gravierenden Fällen — etwa bei Verstößen gegen die Datenverarbeitungsgrundsätze oder bei einer Verarbeitung ohne Rechtsgrundlage. Für Panik besteht also kein Grund. Auf Anfrage von trans aktuell geht auch der Bundesverband Wirtschaft, Verkehr und Logistik (BWVL) davon aus, dass Kontrollbehörden erst nach einer Übergangsfrist kontrollieren und Bußgelder verhängen — wegen der Komplexität der Änderungen.

Wichtig: Künftig ist der Datenschutz bereits in der Entwicklungsphase von Produkten und Dienstleistungen verankert („Privacy by Design“). Das heißt zum Beispiel im Bereich Software: Bereits bei der Entwicklung oder beim Kauf ist die Datenminimierung der Nutzerdaten ein wichtiges Kriterium, wie auch die Pseudonymisierung und Anonymisierung. Außerdem müssen Datennutzer mit Inkrafttreten der EU-DSGVO erweiterte Informationspflichten erfüllen. So ist etwa ein Kunde oder Arbeitnehmer zu informieren, bevor die Daten erhoben werden. Auch den Verwendungshintergrund müssen die Betroffenen erfahren. Zudem ist eine andere Verwendung der erhobenen Daten im Nachhinein nicht mehr möglich. Ebenso verlangt die EU-DSGVO ein Verzeichnis über alle Verarbeitungstätigkeiten. Das Unternehmen muss dieses bei Kontrollen vorlegen. Spezielle Informationspflichten hat der Datennutzer jeweils bei einer Direkterhebung oder Dritterhebung (Art. 13 EU-DSGVO).

Auskunftsrecht

Wie schon nach der bisherigen Rechtslage können Arbeitnehmer Auskunft über gespeicherte personenbezogene Daten verlangen — mit formlosem Antrag und ohne Begründung. Das so genannte Auskunftsrecht ist in Art. 15 der EU-DSGVO detailliert beschrieben. Unternehmen sind gut beraten, sich rechtzeitig und organisatorisch auf eine zügige und korrekte Auskunftserteilung vorzubereiten.

Die Löschung personenbezogener Daten nimmt wie schon bisher auch in der neuen EU-DSGVO einen breiten Raum ein. Bereits jetzt gilt in Deutschland das Recht auf Datenlöschung, **wenn die Speicherung von Daten nicht aus zwingenden vertraglichen oder rechtlichen Gründen erforderlich ist.**

Auch in der neuen EU-DSGVO ist dies als ein „Recht auf Vergessen“ ausdrücklich festgeschrieben. Wenn beispielsweise ein Betroffener seine Einwilligung zur Datenerhebung widerruft und auch keine sonstige Rechtsgrundlage greift, müssen personenbezogene Daten eigenständig durch den Verantwortlichen gelöscht werden (Art. 17 EU-DSGVO), **und zwar unverzüglich.**

Zu viele Öffnungsklauseln

Allerdings: Im Internet ist das Recht auf Vergessen noch nicht geregelt. Bislang stoßen nicht alle Neuerungen in der EU-DSGVO auf durchweg positive Resonanz. So gibt es auch Kritik an der von der EU-Kommission angestrebten Vollharmonisierung des Datenschutzes, die nicht erreicht werde. Es gebe außerdem zu viele Öffnungsklauseln.

Besondere Vorsicht ist geboten, wenn personenbezogene Daten in sogenannte Drittstaaten übermittelt werden sollen, also in Länder außerhalb der Europäischen Union. Die EU-DSGVO sieht dafür besondere Regelungen vor (Art. 9, 44 und 45). So dürfen personenbezogene Daten an ein Drittland nur übermittelt werden, wenn es dort nach Ansicht des Gesetzgebers ein angemessenes Schutzniveau gibt. Ausschlaggebend hierfür sind Kriterien wie Rechtsstaatlichkeit sowie Achtung der Menschenrechte und Grundfreiheiten.

Wichtig zu wissen

- Nur noch kurze Übergangsfrist bis 25. Mai 2018
- Kunde kann die Löschung personenbezogener Daten verlangen. Das Unternehmen muss dem entsprechen.
- Bei Verstößen stehen Bußgelder von bis zu 20 Millionen Euro oder vier Prozent des weltweit erzielten Gesamtumsatzes im Raum.
- Mit der EU-DSGVO tritt am 25. Mai auch das neue Bundesdatenschutzgesetz (BDSG-neu) in Kraft. Dieses orientiert sich stark an der EU-DSGVO, lässt jedoch Spielräume.

Bei der Umsetzung beachten

- Informationspflichten und Löschkonzepte implementieren
- Datenschutzorganisation anpassen
- Meldepflichten organisieren
- Dienstleistungsbeziehungen anpassen
- Dokumentation aufbauen
- IT-Sicherheit anpassen
- Betriebsvereinbarungen anpassen

To-do-Liste bis spätestens 25. Mai

- Prüfen, ob die Informationspflichten gegenüber Betroffenen anhand der bestehenden Datenverarbeitungsprozesse bereits EU-DSGVO-konform eingehalten werden.
- Ist-Zustand im Hinblick auf die aktuellen Prozesse im Unternehmen analysieren, zum Beispiel Dokumentation sowie Betriebsvereinbarungen. Anschließend eine Lückenanalyse zwischen Ist- und Soll-Zustand erstellen und abarbeiten.
- Technische und operative Abläufe prüfen — zum Beispiel bei der Reaktion auf Datenlecks. Wegen der sehr kurzen

gesetzlichen Meldefrist von nur 72 Stunden am besten ein Krisenmanagement verankern.

- Vollständiges Verzeichnis von Verarbeitungstätigkeiten erstellen. Dieses Verzeichnis dient als Grundlage für eine strukturierte Datenschutzdokumentation.
- Betrieblichen Datenschutzbeauftragten (DSB) benennen.
Dadurch sollte die Koordination der datenschutzrechtlichen Belange des Unternehmens in einer Position verankert werden, sofern noch nicht geschehen.

Der DSB kann auch von einem externen Dienstleister gestellt werden. Diese Vorgehensweise schützt den Arbeitgeber vor dem erweiterten Kündigungsschutz in Bezug auf dessen Position als DSB.