8MAN

Access Rights Management. Only much Smarter.

EU-DATENSCHUTZ:
DIE DS-GVO NEUERUNGEN IN KÜRZE

Protected Networks

EU-DATENSCHUTZ: DIE DS-GVO NEUERUNGEN IN KÜRZE

Das ändert sich mit dem neuen Recht

Mit der neuen EU-Datenschutz-Grundverordnung (EU-DS-GVO) soll das europäische Datenschutzrecht vereinheitlicht werden. Es ist eher ein Rechtskonstrukt zwischen Richtlinie und Verordnung. Der neue EU-Datenschutz wird deutlich strenger als das bisherige deutsche Recht. Es sieht aber vor, dass für eine Reihe von Themen Abweichungen zur Harmonisierung mit nationalem Recht möglich sind.

Weltweite Geltung

Die Verordnung soll nicht nur in der gesamten Union gelten. Auch Unternehmen im Ausland müssen den europäischen Datenschutz anwenden, wenn sie Daten von Personen in der EU verarbeiten, um diesen Personen Waren oder Dienstleistungen anzubieten oder das Verhalten von Personen in der Union beobachten.

Wann tritt die Neuregelung in Kraft?

Verabschiedet am 14. April 2016; Anwendung findet sie nach dem derzeitigen Planungsstand im ersten Quartal 2018.

Bußgelder bis zwei Prozent vom Umsatz bei leichten Fehlern

Es drohen Geldbußen von bis zu zwei Prozent des Jahresumsatzes, wenn Unternehmen es versäumen, Verarbeitungsvorgänge ordnungsgemäß zu dokumentieren (Artikel 28), die Aufsichtsbehörde und betroffene Personen über Datenschutzverletzungen zu informieren (Artikel 31 und 32) oder Datenschutz-Folgenabschätzungen (siehe auch Absatz weiter unten) durchzuführen (Artikel 33).

Starke Sanktion von bis zu vier Prozent des Jahresumsatzes bei Versäumnis

Als ernsthafter Verstoß gilt dabei die Nichteinhaltung der Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten (Artikel 5) sowie der Bestimmungen zur Einwilligung betroffener Personen (Artikel 7). Dabei handelt es sich im Grunde um Verstöße gegen die gesetzlich verankerten „Privacy-by-Design Prinzipien" (Datenschutz durch Technik, siehe auch Absatz weiter unten), die sicherstellen sollen, dass Datenschutz und Privatsphäre schon in der Entwicklung von Technik beachtet werden. Um dabei auch besser vor Übergriffen durch Datenkraken zu schützen.

Persönliche Haftung von Datenschützern und Managern

Bisher mussten deutsche Datenschutzbeauftragte lediglich auf das Einhalten der Vorschriften „hinwirken". Nach dem neuen Recht müssen jetzt auch Manager, Datenschutzbeauftragte, IT-Chefs aufpassen und überwachen, dass sämtliche Regeln auch wirklich eingehalten werden. Auch Vorstände oder Geschäftsführer sind betroffen. Sie haben schon nach dem bisherigen Recht weitreichende Kontrollpflichten. Hält sich eine Führungskraft nicht an die neuen Regeln, drohen Bußgelder von bis zu 20 Millionen Euro. Dazu kommt die persönliche Haftung, wenn das Unternehmen wegen eigenen Fehlern Geldbußen oder Schadensersatzforderungen bezahlen muss. Durch die drastisch gestiegenen Risiken können Nachlässigkeiten künftig sehr schnell den Arbeitsplatz kosten.

Neue Meldepflichten mit 72 Stunden Meldefrist

In Artikel 31 der DS-GVO ist geregelt, dass eine Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde zu melden ist, unter der Bedingung, dass die Verletzung zu einem Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen führen kann.

Training, Nachweispflichten und Rechenschaft

Unternehmen müssen wirksame Datenschutz-Richtlinien einführen und ihre Mitarbeiter im neuen Recht schulen. Es reicht nicht, sich nur an die neuen Vorschriften zu halten, es muss auch der Nachweis durch Dokumentation erbracht werden (z.B. Reporte). Diese unscheinbare Veränderung kann in der Praxis sehr teuer werden. Denn den geforderten Beweis, dass man alles richtig gemacht hat – und das während eines Prozesses über Bußgelder oder Schadensersatz – muss ein Unternehmen erst einmal erbringen können. Voraussetzung hierfür: ein effektives Datenschutz Management System – inklusive Risikoanalysen, Trainings, Strukturen, Prozesse, Kontrollen und ein schnelles Change Management beim Datenschutz.

Information und Unterrichtung

Unternehmen müssen Personen künftig viel umfassender und früher unterrichten, wenn sie deren Daten verarbeiten. Bei Fehlern drohen hohe Bußgelder.

Recht auf Vergessenwerden

Werden personenbezogene Daten nicht mehr benötigt, müssen sie gelöscht werden. Wenn Daten veröffentlicht wurden, muss der Empfänger, an den die Daten weitergegeben wurden, darüber informiert werden, wenn ein Betroffener die Löschung von Links oder Kopien dieser Daten verlangt.

Recht auf Kopie und „Datenportabilität"

Ein Betroffener kann von Unternehmen, die seine Daten speichern, verlangen, dass sie ihm eine Kopie sämtlicher gespeicherter Daten geben. Das wird teuer und aufwändig für die Wirtschaft.

Koppelungsverbot bei Einwilligungen

Vertragliche Zusatzleistungen dürfen nicht mehr daran geknüpft werden, dass der Betroffene in die Verarbeitung seiner Daten einwilligt. Das Geschäftsmodell „Dienste gegen Daten" könnte dadurch „erschwert" werden.

Datenschutz-Folgenabschätzungen

Wenn eine Datenverarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge hat, muss das Unternehmen eine umfassende Vorprüfung vornehmen, den Vorgang dokumentieren und gegebenenfalls später mit der Datenschutzbehörde abstimmen.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Unternehmen müssen ihre IT-Systeme so gestalten, dass diese den Anforderungen der Verordnungen entsprechen, d.h. beispielsweise von vornherein nur so wenige Daten sammeln und verarbeiten, wie es zur Erreichung des konkret verfolgten Zwecks (Zweckbindung) notwendig ist. Sofern möglich, sollen Daten pseudonymisiert werden. Stellt ein Unternehmen nicht die vorgeschriebene Datensicherheit sicher – beispielsweise zur Abwehr von Hackerangriffen - drohen bei Mängeln Bußgelder von bis zu zwei Prozent des Umsatzes.

Datenschutz am Arbeitsplatz

Viele der neuen Regeln hatten die IT-Wirtschaft im Blick und passen daher schlecht zum Datenschutz am Arbeitsplatz. Allerdings kann man in Betriebsvereinbarungen alternative Vorgaben zur Verarbeitung von Arbeitnehmerdaten vereinbaren. Das geht aber nur zusammen mit dem Betriebsrat. Daher verhandeln die ersten Unternehmen jetzt schon mit ihren Arbeitnehmervertretern.

Checkliste für Entscheider

Unternehmen sollten einen Fahrplan erstellen, wie sie die neuen Anforderungen bis 2018 erfüllen. Einige Arbeitsschritte liegen dabei schon jetzt auf der Hand:

- Gefährdungsanalyse: Welche Risiken drohen dem eigenen Geschäftsmodell, wie hoch sind die Umsätze des Unternehmens, welche Bußgeldrisiken oder sonstigen Nachteile drohen?
- Compliance-Review: Unterzieht sich das Unternehmen einer Überprüfung der Compliance-Richtlinien (Auditing), um die Rechtmäßigkeit des Unternehmenshandelns (rechtlich, behördlich und unternehmensintern) sicherzustellen?
- Lücken-Analyse: Wo steht das Unternehmen heute, welche Schritte sind nötig, um künftig die Anforderungen des neuen EU-Datenschutzrechts zu entsprechen?
- Ressourcenplanung: Welche Mittel brauche ich für die Umstellung auf das neue Recht, welche Ressourcen sind verfügbar, wo fehlt etwas?
- Budgetplanung: Für Datenschutz muss auch Geld in die Hand genommen werden. Bei den Budgetverhandlungen wird auch die Haftung des Unternehmens, aber auch der Entscheidungsträger keine kleine Rolle spielen.
- Projektplanung: Gerade für große Unternehmen oder gar Konzerne kann die Transformation auf das neue EU-Recht ein Mammutprojekt sein. Dementsprechend sollte auch die Projektplanung von Anfang an professionell und flexibel sein. Allein die Liste der beteiligten Unternehmensfunktionen ist deutlich länger als bei vielen anderen Großprojekten.
- Dienstleister: Wen ziehe ich als Unternehmen für die Neustrukturierung meiner Unternehmensprozesse und IT-Systeme zu Rate? Zertifizierte Datenschutzberater, IT-Sicherheit-Beratung oder IT-Sicherheit Systemhaus?

Quellen:

https://www.bvdnet.de

http://blog.wiwo.de

http://www.bvdw.org