TechTarget

E-Guide

EU-Datenschutz-Grundverordnung: Was sich für Unternehmen ändert

Inhalt

Unternehmen in Deutschland sollten nicht glauben, dass ihre aktuellen Maßnahmen nach Bundesdatenschutzgesetz (BDSG) bereits so umfangreich sind, dass bei Inkrafttreten der geplanten EU-Datenschutz-Grundverordnung keine zusätzlichen Aufgaben auf sie zukommen. In Wirklichkeit stehen so einige Änderungen ins Haus. Einen ersten Überblick bieten zum Beispiel die Stellungsnahmen der Aufsichtsbehörden für den deutschen Datenschutz oder des Branchenverbandes BITKOM.

Lesen Sie hier alles über die Änderungen in der EU-Datenschutz-Grundverordnung und erfahren Sie, worauf sich Ihr Unternehmen in Zukunft einstellen muss.

(Article dotted line)

EU-Datenschutz-Grundverordnung: Was sich für Unternehmen ändert

Oliver Schonschek

Unternehmen in Deutschland sollten nicht glauben, dass ihre aktuellen Maßnahmen nach Bundesdatenschutzgesetz (BDSG) bereits so umfangreich sind, dass bei Inkrafttreten der geplanten EU-Datenschutz-Grundverordnung keine zusätzlichen Aufgaben auf sie zukommen. In Wirklichkeit stehen so einige Änderungen ins Haus. Einen ersten Überblick bieten zum Beispiel die Stellungsnahmen der Aufsichtsbehörden für den deutschen Datenschutz oder des Branchenverbandes BITKOM.

Neben den noch diskutierten Themen wie dem genauen Anwendungsbereich der Datenschutz-Grundverordnung, der Fragen hinsichtlich Einwilligung der Betroffenen, der Umsetzung der Auftragsdatenverarbeitung und Auftragskontrolle zum Beispiel bei Cloud Computing, dem Datenaustausch zwischen verbundenen Unternehmen, der Profilbildung und dem Recht auf Vergessenwerden gibt es auch geplante Änderungen, die eher kaum

diskutiert werden und deren Umsetzung mit großer Wahrscheinlichkeit ansteht.

Inhalt

Eine Abwartehaltung, ob bestimmte Compliance-Forderungen tatsächlich kommen, kann sich zum Problem entwickeln: Die geplante Datenschutz-Grundverordnung der EU wird nach Verabschiedung ohne Übergangsfrist in Kraft treten, muss also nicht mehr in nationales Recht übertragen werden. Dies macht die Zeitspanne für mögliche Umstellungen und Änderungen in Unternehmen mehr als gering.

Datenschutzaufgaben sollten vorbereitet werden

Nach Artikel 22 (Pflichten des für die Verarbeitung Verantwortlichen) werden Unternehmen auch in Zukunft durch geeignete Strategien und Maßnahmen sicherstellen müssen, dass personenbezogene Daten in Übereinstimmung mit dem Datenschutzrecht verarbeitet werden. Gut geplant sein wollen die Nachweise dieser Strategien und Maßnahmen, denn Nachweise werden explizit gefordert.

Zu den erforderlichen Maßnahmen nach Artikel 22 gehören eine Datenschutz-Dokumentation, technisch-organisatorische Maßnahmen der Datensicherheit, Risikoanalysen (Datenschutz-Folgeabschätzungen genannt), die Umsetzung von Anforderungen für Genehmigungen oder Konsultationen der Aufsichtsbehörden und die Benennung eines Datenschutzbeauftragten.

Dokumentation des Datenschutzes ist Pflicht

Die Verfahren der Datenverarbeitung und die internen Maßnahmen zur Erfüllung der Datenschutz-Forderungen müssen dokumentiert werden (Artikel 28), etwa in internen Datenschutz-Berichten. Erfahrungsgemäß ist die Aufstellung solcher Berichte recht zeitaufwändig, so dass Unternehmen nicht zu spät mit entsprechenden Vorbereitungen beginnen sollten.

Wichtig dabei ist auch, dass die Qualität und die Einhaltung der dokumentierten Maßnahmen für den Datenschutz regelmäßig überprüft werden müssen. Unternehmen in Deutschland kennen die Dokumentationsvorgaben bereits von dem sogenannten

Inhalt

Verfahrensverzeichnis. Zusätzlich zu den Verfahren dokumentiert werden müssen die Datenschutz-Folgeabschätzung und die Maßnahmen der Datensicherheit.

Datensicherheit auch für neue Technologien

Die technischen und organisatorischen Maßnahmen für die Datensicherheit sollen grundsätzlich auf Basis einer Risikobewertung erfolgen (Artikel 30). Diese Risikobewertung sollte ebenso im Sinne von Compliance-Nachweisen dokumentiert sein wie die daraus resultierenden Sicherheitsmaßnahmen. Die geplanten und umgesetzten Sicherheitsmaßnahmen sollen dabei den aktuellen Stand der Technik „für bestimmte Sektoren und Datenverarbeitungssituationen“ sowie die technologische Entwicklung berücksichtigen.

Unternehmen werden den Stand der Technik und die technologische Entwicklung nicht ohne weiteres umfassend kennen und bewerten können. Eine frühzeitige und regelmäßige Risiko-Analyse und Datenschutz-Folgeabschätzung ist deshalb angeraten.

Folgen der Datenverarbeitung frühzeitig abschätzen

Die Datenschutz-Grundverordnung nennt konkrete Fälle von Datenverarbeitung, bei der Risiko-Analysen vorzusehen sind, wie

- die systematische und umfassende Auswertung persönlicher Aspekte einer natürlichen Person, beispielsweise zwecks Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens,
- die Verarbeitung von Daten über das Sexualleben, den Gesundheitszustand, die Rasse oder die ethnische Herkunft oder für die Erbringung von Gesundheitsdiensten, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder ansteckende Krankheiten, wenn die betreffenden Daten in großem Umfang im Hinblick auf Maßnahmen oder Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen,

- die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels Videoüberwachung,
- sowie die Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten.

Unternehmen sollten sich ihre Verfahren schon jetzt nochmals genau ansehen und sich auf die Risiko-Bewertung für entsprechende Fälle von Datenverarbeitung vorbereiten. Eine Beschäftigung mit diesen Compliance-Vorgaben lohnt sich schon heute in mehrfacher Hinsicht: zur Vorbereitung auf die geplante EU-Datenschutz-Grundverordnung, für die Erfüllung des bis zum Inkrafttreten der EU-Datenschutz-Grundverordnung gültigen Bundesdatenschutzgesetzes sowie zur weiteren Optimierung des eigenen Datenschutz-Managements.

Inhalt

Privacy by Design im EU-Datenschutz: Was Unternehmen wissen sollten

Oliver Schonschek

In der IT-Sicherheit spricht man oftmals von der „Schwachstelle Mensch“. Darunter versteht man Fehler der Nutzer, die ungewollt zu einem Sicherheitsrisiko beitragen. Im Datenschutz gibt es ein ähnliches Phänomen: IT-Anwender lassen viele Möglichkeiten ungenutzt, ihre personenbezogenen Daten besser zu schützen.

Es steckt kein böser Wille dahinter, wenn die Nutzer Daten unzureichend schützen. In Umfragen, zum Beispiel von BITKOM, wird immer wieder deutlich, dass den Nutzern der Datenschutz wichtig ist. Gleichzeitig zeigen die Studien aber, dass wichtige Sicherheitsmaßnahmen wie die Verschlüsselung von E-Mails kaum genutzt werden. Der Schluss liegt nahe, dass die meisten Nutzer durch die Vorgaben des Datenschutzes überfordert sind. Aus diesem Grund werden vom Datenschutz höhere Erwartungen an die Administratoren und an die IT-Anbieter gestellt.

Inhalt

Datenschutz nimmt Anbieter und Administratoren stärker in die Pflicht
Datenschützer fordern seit längerem schon, den Schutz personenbezogener Daten so früh wie möglich in IT-Lösungen zu berücksichtigen. Bereits in der Konzeption und Entwicklung, aber auch in den Voreinstellungen soll der Datenschutz einen wichtigen Stellwert einnehmen. So sollen die Nutzer später bei der Umsetzung von Datensicherheitsmaßnahmen unterstützt werden oder aber nahezu gar nicht mehr anders können, als den Datenschutz zu beachten. Man spricht von „Privacy by Design“ und „Privacy by Default“. Beide Datenschutz-Prinzipien richten sich an die IT-Anbieter. Der Datenschutz als Voreinstellung (“by Default”) wendet sich zusätzlich an die Administratoren in den Anwenderunternehmen.

IT-Anbieter sollten ausgesprochene Datenschutzfunktionen beziehungsweise datenschutzfreundliche Funktionen in ihren Lösungen vorsehen. Das fordern die Aufsichtsbehörden in einer entsprechenden Entschließung als generelles Prinzip und nennen „Privacy by Design“ auch exemplarisch als Anforderung bei Lösungen im Bereich Webtracking und bei der App-Entwicklung. Aber auch die geplante Datenschutz-Grundverordnung der EU sieht einen eigenen Artikel zu Privacy by Design und Privacy by Default vor, dort „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen“ (Artikel 23) genannt.

Anwender sollen Lösungen nach Datenschutzaspekten auswählen
Die EU-Datenschutz-Grundverordnung wird von Anwenderunternehmen verlangen, dass nur Verfahren eingesetzt werden, die sicherstellen, dass grundsätzlich ausschließlich solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden. Es sollen vor allem nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke unbedingt nötig ist. Diese Daten sollen auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Inhalt

Damit sind Anwenderunternehmen insbesondere gehalten, ihre IT-Lösungen und Verfahren so auszuwählen, dass die Prinzipien der Datensparsamkeit, Datenvermeidung, Zweckbindung, fristgerechten Löschung von Daten und Zugangs- und Zugriffskontrolle umgesetzt werden. Das kann nicht alleine durch technische Maßnahmen erfolgen, wird aber durch technische Maßnahmen deutlich vereinfacht. Somit sollten Anwenderunternehmen gezielt solche Verfahren und Lösungen wählen und einsetzen, die die Datenschutz-Prinzipien unmittelbar beachten, also Privacy By Design und Privacy By Default bieten.

Datenschutz gehört ins Lastenheft und ins Pflichtenheft

Wenn Anbieter neue Produkte entwickeln oder bestehende weiterentwickeln, sollte der Datenschutz Teil des Pflichtenheftes werden. Anwenderunternehmen sollten ebenfalls den Datenschutz als festen Bestandteil des Lastenheftes begreifen. Für alle IT-Lösungen, die personenbezogene Daten verarbeiten sollen, gehören neben den rein fachlichen Anforderungen auch die Forderungen nach sparsamer Datenerfassung und Datenspeicherung, nach Vermeidung missbräuchlicher Datennutzung, nach intelligenten Löschfunktionen, sicherem Zugangsschutz und einem ausreichend ausgefeiltem Berechtigungssystem hinzu.

Gerade die Verschlüsselung spielt bei vielen dieser Forderungen eine wichtige Rolle. Für das eingangs erwähnte Beispiel oftmals fehlender Verschlüsselung bedeutet dies, dass Unternehmen Lösungen bevorzugen sollten, die integrierte Verschlüsselungsfunktionen bieten oder diese einfach integrieren lassen. Dabei sollte die Verschlüsselung bereits so voreingestellt werden, dass die einzelnen Nutzer möglichst automatisch die personenbezogenen Daten schützen. IT-Anbieter sollten ihre Lösungen entsprechend mit Schnittstellen für Sicherheitslösungen und mit Datenschutz-Optionen versehen, die es einfacher machen, den Datenschutz zu beachten und nicht etwa komplizierter.

Inhalt

Kostenlose Onlineressourcen für IT-Experten

TechTarget publiziert qualifizierte Medieninhalte im IT-Bereich, die Ihren Informationsbedarf bei der Suche nach neuen IT-Produkten und Technologien decken und Ihr Unternehmen somit gezielt in der Strategieentwicklung unterstützen. Es ist unser Ziel, Ihnen durch die Bereitstellung von Onlineressourcen zu den aktuellsten Themen der IT-Branche die Kaufentscheidungen für IT-Produkte zu erleichtern und kostengünstiger zu gestalten.

Unser Netzwerk an technologiespezifischen Webseiten erlaubt es Ihnen, auf eine der weltweit größten Onlinebibliotheken zum Thema IT zuzugreifen und anhand von unabhängigen Expertenmeinungen und Analysen, zahlreichen Whitepapern, Webcasts, Podcasts, Videos, virtuellen Messen und Forschungsberichten zu ausgewogeneren Kaufentscheidungen zu gelangen.

Unsere Onlineressourcen berufen sich auf die umfangreichen Forschungs- und Entwicklungskompetenzen führender Technologieanbieter und ermöglichen es Ihnen somit, Ihr Unternehmen für künftige Marktentwicklungen und –herausforderungen zu rüsten. Unsere Live-Informationsveranstaltungen und virtuellen Seminare geben Ihnen die Möglichkeit, Ihre täglichen individuellen Herausforderungen im Bereich IT mit herstellerunabhängigen Experten zu diskutieren.

Desweiteren können Sie in unserem Social Network, dem IT Knowledge Exchange, praxisnahe Erfahrungsberichte mit Fachkollegen und Experten in Echtzeit austauschen.

Was macht TechTarget so einzigartig?

Bei TechTarget steht die Unternehmens-IT im Mittelpunkt. Unser Redaktions- und Autorenteam und unser breites Netzwerk an Industrieexperten bietet Ihnen Zugriff auf die neuesten Entwicklungen und relevantesten Themen der Branche.

Inhalt

TechTarget liefert klare und überzeugende Inhalte und umsetzbare Informationen für die Profis und Entscheidungsträger der IT-Branche. Wir nutzen die Schnelligkeit und Unmittelbarkeit des Internets um Ihnen in realen und virtuellen Kommunikationsräumen hervorragende Networking-Möglichkeiten mit Fachkollegen zur Verfügung zu stellen.

Weitere deutsche TechTarget Webseiten:

- SearchDataCenter.de
- SearchEnterpriseSoftware.de
- SearchNetworking.de
- SearchSecurity.de
- SearchStorage.de