Martin Schweinoch

Datenschutz fordert IT-Sicherheit

Die Datenschutz-Grundverordnung der Europäischen Union setzt zum 25.05.2018 neue Regeln für den Schutz personenbezogener Daten. Dies betrifft nicht nur Fragen, wer unter welchen Bedingungen welche Daten zu welchen Zwecken nutzen darf. Sondern dies betrifft gerade auch Anforderungen an die IT-Sicherheit, die einem risikobasierten Ansatz folgen.

Was sind überhaupt „personenbezogene Daten“?

So harmlos der Begriff „personenbezogene Daten“ klingen mag, so umfassend ist er zu verstehen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das reicht von Name und Anschrift – die sich offensichtlich auf eine Person beziehen – bis zu Informationen, deren Personenbezug man auf den ersten Blick nicht vermuten würde. Der Europäische Gerichtshof versteht auch dynamische IP-Adressen, die ein Nutzer beim Besuch einer Webseite im Internet verwendet, als personenbezogene Daten aus Sicht des Betreibers der Webseite. Zwar erkennt der Betreiber der Webseite nur die IP-Adresse, aber aus bei ihm vorliegenden Informationen nicht die Person des Nutzers. Unter bestimmten Umständen könnte der Webseitenbetreiber aber von dem Anbieter des Internetzugangs eine Auskunft verlangen, welchem Kunden als Nutzer die verwendete IP-Adresse zum Zeitpunkt des Webseitenbesuchs zugeordnet war. Nach Auffassung des Europäischen Gerichtshofs reicht schon diese Möglichkeit für den Webseitenbetreiber, unter bestimmten Voraussetzungen die Person des Nutzers in Erfahrung zu bringen, um die Anwendung der Datenschutzvorschriften zu bejahen. Mit dem entsprechenden Urteil (EuGH vom 19.10.0216 – C-582/14) ist diese Frage letztinstanzlich abschließend entschieden.

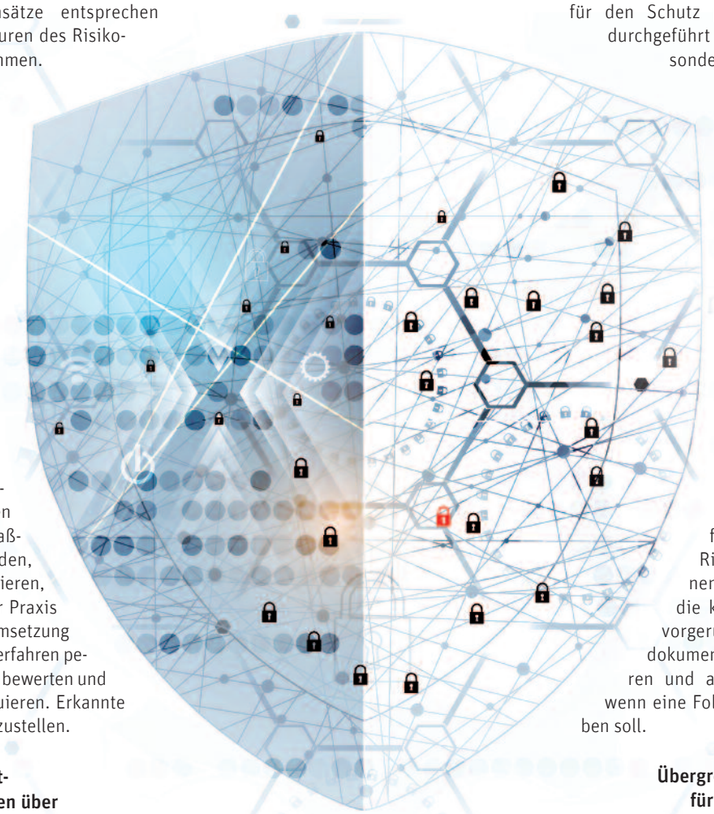
Für die Unternehmenspraxis bedeutet das eine quasi umgekehrte Fragestellung: Nachdem sehr viele Daten in einem Unternehmen zumindest irgendeinen – auch nur mittelbaren – Bezug zu einer natürlichen Person (Kunde, Mitarbeiter, etc.) aufweisen, ist in der Praxis zu fragen, ob für konkret verwendete Daten ausnahmsweise kein solcher Personenbezug vorliegt. Der Datenschutz hat in Unternehmen also einen wesentliche breiteren Anwendungsbereich, als es auf den ersten Blick erscheinen würde.

Risikobasiertes IT-Sicherheitskonzept

Die Datenschutz-Grundverordnung verlangt für alle personenbezogenen Daten ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen, das sich – grob ausgedrückt – an den Risiken der Datenverarbeitung für die betroffene Person orientieren muss (Art. 32 Abs. 1 DS-GVO). Für die Beurteilung, welches Schutzniveau erforderlich ist, ist eine Vielzahl von Faktoren einzubeziehen: Der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung gehören ebenso dazu wie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte betroffener Personen. Damit eröffnet diese Regelung den Verarbeitern personenbezogener Daten einerseits Ermessens- und Beurteilungsspielräume. Anderseits sind diese Spielräume auch tatsächlich auszufüllen, da der Verarbeiter für den ordnungsgemäßen Umgang mit personenbezogenen Daten dokumentiert Rechenschaft ablegen muss (Art. 5 Abs. 2 DS-GVO). Für unterschiedliche Verarbeitungen verschiedener personenbezogener Daten können da pauschale Beurteilungen oder Antworten nicht genügen. Vielmehr ist ein IT-Sicherheitskonzept gefordert, das den unterschiedlichen Risiken angemessene Maßnahmen entgegensetzt.

Solche Schutzmaßnahmen können technischer und organisatorischer Natur sein. Dazu gehören etwa die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste; die Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten bei physischen oder technischen Zwischenfällen und – nicht zuletzt – notwendige Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen. Diese Ansätze entsprechen bereits bewährten Strukturen des Risikomanagements in Unternehmen.

Die Umsetzung erfordert zunächst eine Bewertung von Risiken der Verarbeitung personenbezogener Daten aus datenschutzrechtlicher Sicht. Eine solche Risikobewertung besteht aus mehreren relevanten Faktoren und führt üblicherweise zur Einstufung der jeweiligen Verarbeitung in eine definierte Schutzklasse (etwa niedrig – mittel – hoch). Jeder Schutzklasse können definierte Anforderungen an die technischen und organisatorischen Maßnahmen zugeordnet werden, die nicht nur zu dokumentieren, sondern dann auch in der Praxis umzusetzen sind. Diese Umsetzung ist durch dokumentierte Verfahren periodisch zu überprüfen, zu bewerten und ihre Wirksamkeit zu evaluieren. Erkannte Defizite sind natürlich abzustellen.



Pflichtinformationen über Datenschutzverstöße

Die Datenschutz-Grundverordnung schreibt zukünftig Pflichtinformationen über aufgetretene Datenschutzverstöße nicht nur an die Aufsichtsbehörden vor. Vielmehr sind auch die betroffenen Personen über aufgetretene Datenschutzverstöße zu informieren.

Wer für die Verarbeitung personenbezogener Daten als Verantwortlicher tätig ist, muss Verletzungen des Schutzes personenbezogener Daten möglichst innerhalb von 72 Stunden nach Kenntnis der zuständigen Aufsichtsbehörde melden. Diese Meldung kann er nur unterlassen, wenn voraussichtlich kein Risiko für die Rechte betroffener Personen besteht. Diese Pflichtmeldung muss nähere Angaben über die Schutzverletzung und soweit möglich die betroffenen Daten und die Zahl der betroffenen Personen enthalten. Auch die wahrscheinlichen Folgen der Schutzverletzung sind zu beschreiben zusammen mit ergriffenen oder vorgeschlagenen Maßnahmen zur Beseitigung der Schutzverletzung und Abmilderung möglicher Folgen. Das Unterlassen solcher Pflichtmitteilungen ist durch ganz erhebliche Bußgelder bedroht, die bis zu 10 Millionen Euro oder – wenn höher – bis zu 2 % eines weltweiten Jahresumsatzes eines Unternehmens betragen können. Schon deswegen empfiehlt es sich dringend, unternehmensintern entsprechende Meldeverfahren einzuführen und auch zu testen.

Wenn aufgrund einer Schutzverletzung voraussichtlich ein hohes Risiko für die Rechte der betroffenen Personen besteht, müssen auch diese Personen unverzüglich von der Verletzung informiert werden. Auch dabei sind die wahrscheinlichen Folgen der Verletzung, ein Ansprechpartner im entsprechenden Unternehmen und eine Beschreibung der ergriffenen Maßnahmen zur Behebung der Schutzverletzung oder zur Abmilderung ihrer Folgen mitzuteilen. Diese Meldung kann sich ein Verantwortlicher nur dann ersparen, wenn entsprechende technische und organisatorische Sicherheitsvorkehrungen umgesetzt wurden, die personenbezogene Daten gegen unbefugten Zugriff durch Dritte sicher schützen (etwa Verschlüsselung) oder durch anschließende Maßnahmen sichergestellt wurde, dass kein hohes Risiko für die Rechte der betroffenen Personen besteht. Auch ein Unterlassen solcher Pflichtinformationen an betroffene Personen ist mit ganz erheblichem Bußgeld bedroht.

Pflicht zu Datenschutz-Folgenabschätzung

Wenn eine bestimmte Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte davon betroffener Personen bedeutet, muss vorab eine Abschätzung möglicher Folgen für den Schutz personenbezogener Daten durchgeführt werden. Das trifft insbesondere für die Verwendung neuer Technologien zu. Eine solche Datenschutz-Folgenabschätzung kann – je nach Art der Verarbeitung – mit mehr oder weniger großem Aufwand verbunden sein. Sie folgt in Struktur und Logik den üblichen Mechanismen des Risk-Managements in Unternehmen, allerdings aus dem Blickwinkel des Datenschutzes.

Zunächst ist im Unternehmen aber durch entsprechende Bewertungen festzustellen, ob ein hohes Risiko für den Schutz personenbezogener Daten durch die konkrete Verarbeitung hervorgerufen wird. Auch dafür sind dokumentierte Kriterien zu definieren und anzuwenden, insbesondere wenn eine Folgenabschätzung unterbleiben soll.

Übergreifender Ansatz für IT-Security

Die Datenschutz-Grundverordnung verpflichtet zur Umsetzung eines ganzheitlichen, risikobasierten Ansatzes für die IT-Sicherheit – jedenfalls aus Sicht des Datenschutzes. Viele Unternehmen sind unabhängig davon im eigenen Interesse gut beraten, auch für alle anderen Daten einen risikobasierten Ansatz für die IT-Security umzusetzen. Schließlich sind die Daten heute wichtiges Produktionsmittel für viele Unternehmen und zudem schützenswertes Know How.

Den gesetzlichen Anforderungen des Datenschutzes wird aber nur ein dokumentiertes Konzept für die IT-Security personenbezogener Daten gerecht, das auch dokumentiert umgesetzt worden ist.

Die Datenschutz-Grundverordnung gilt ab 25.05.2018 – also quasi übermorgen. Für die Umsetzung eines IT-Security Konzepts oder die Dokumentation vorhandener Konzepte drängt nun die Zeit. ◀