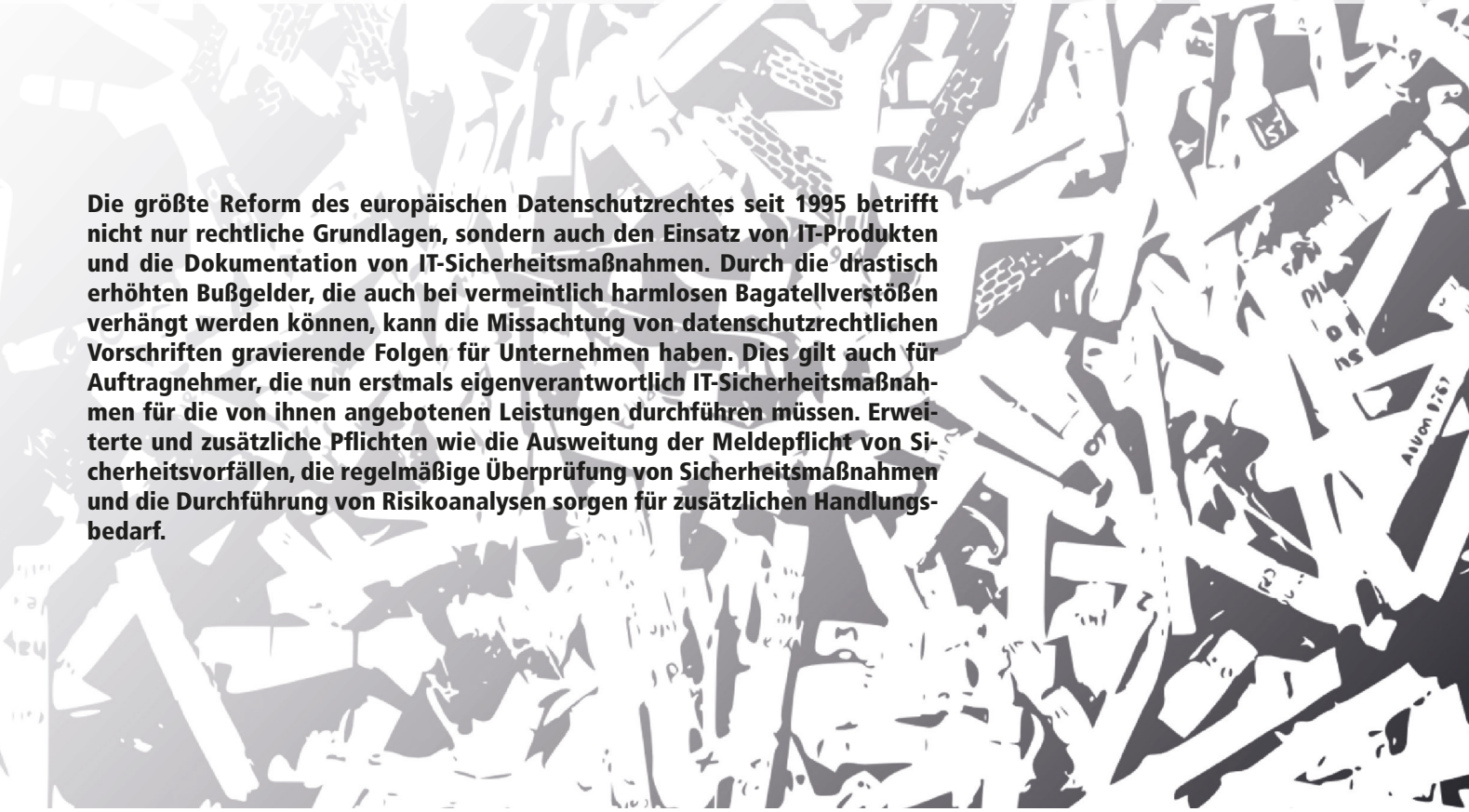
Konsequenzen aus der neuen EU-Datenschutz-Grundverordnung (Teil 1)

Mehr gesetzliche Pflichten für IT-Verantwortliche



Die größte Reform des europäischen Datenschutzrechtes seit 1995 betrifft nicht nur rechtliche Grundlagen, sondern auch den Einsatz von IT-Produkten und die Dokumentation von IT-Sicherheitsmaßnahmen. Durch die drastisch erhöhten Bußgelder, die auch bei vermeintlich harmlosen Bagatellverstößen verhängt werden können, kann die Missachtung von datenschutzrechtlichen Vorschriften gravierende Folgen für Unternehmen haben. Dies gilt auch für Auftragnehmer, die nun erstmals eigenverantwortlich IT-Sicherheitsmaßnahmen für die von ihnen angebotenen Leistungen durchführen müssen. Erweiterte und zusätzliche Pflichten wie die Ausweitung der Meldepflicht von Sicherheitsvorfällen, die regelmäßige Überprüfung von Sicherheitsmaßnahmen und die Durchführung von Risikoanalysen sorgen für zusätzlichen Handlungsbedarf.

Der 15. Dezember 2015 markiert den Höhepunkt eines bemerkenswerten Gesetzesvorhabens, das Unternehmen aller Größen und Branchen sowie Vereine, Verbände und auch die öffentliche Verwaltung betrifft. Mehr als 3.000 Änderungsanträge (1), intensive Lobby-Arbeit und lange Verhandlungen begleiteten das Projekt, dem der Film „Democracy – Im Rauch der Daten" (2) ein Denkmal gesetzt hat. Das Gesetz ist aus zwei Gründen bemerkenswert:

- zum ersten Mal regelt die EU ein Rechtsgebiet unmittelbar fast abschließend und
- beansprucht Geltung auch für aus dem Ausland heraus auf dem europäischen Markt operierende Unternehmen.

Die unmittelbare Geltung bedeutet, dass mit Blick auf die für Unternehmen relevanten Vorschriften der nationale Gesetzgeber eine Umsetzung oder Anpassung an nationales Recht weder vornehmen muss noch darf. Der EU-Gesetzestext gilt unmittelbar. Die bisher bestehenden nationalen Regelungen werden obsolet.

Der Gesetzestext, „Datenschutz-Grundverordnung" (kurz: DS-GVO) genannt, liegt als Verhandlungsergebnis zwischen EU-Kommission, EU-Parlament und EU-Rat vor (3). Er wird vor der in Kürze erwarteten offiziellen Verabschiedung durch das EU-Parlament und den EU-Rat redaktionell überarbeitet und übersetzt. Inhaltliche Änderungen sind erfahrungsgemäß nicht zu erwarten. Nach der offiziellen Verabschiedung durch das EU-Parlament und den EU-Rat tritt die DS-GVO 20 Tage nach Verkündung im Amtsblatt in Kraft. Vollzogen wird sie jedoch erst zwei Jahre später. In dieser Übergangszeit gilt das bisherige Datenschutzrecht, insbesondere das Bundesdatenschutzgesetz (BDSG), unverändert weiter.

Zwei Jahre bis zum Vollzug – eine knappe Zeitspanne

Eine zweijährige Übergangsfrist erscheint üppig bemessen und lädt ein, die Beschäftigung mit der DS-GVO um 23 Monate zu verschieben. Dies ist gleichsam ein gefährlicher Trugschluss, da die DS-GVO Änderungen in zahlreichen Bereichen der betrieblichen Organisation, insbesondere in folgenden Bereichen bedingt:

- Rechtsgrundlagen (Welche Datenverarbeitung ist erlaubt und welche verboten?),
- Rechte der Bewerber und Mitarbeiter,
- Dokumentationspflichten,

» IT-Sicherheit,
» Beziehungen zu Dienstleistern und
» Haftung & Bußgelder.

Die neuen Vorgaben sowie die Bußgeldandrohung richten sich an alle Unternehmen. Dienstleister im Rahmen einer Auftragsdatenverarbeitung, wie zum Beispiel Cloud-Dienste, Administration oder Nutzerverwaltung, müssen zukünftig in eigener Verantwortung und Initiative die unten dargestellten Sicherheitsmaßnahmen ergreifen (4). Ein Warten auf die Anweisungen eines Auftraggebers ist im Unterschied zu heute nicht zulässig.

Ein vollständiger Überblick würde den Rahmen des Beitrags – sogar des Heftes – sprengen, deshalb konzentriert sich dieser Beitrag auf ausgewählte Auswirkungen für die IT-Sicherheit.

Dokumentation ein Insolvenzrisiko?

Die DS-GVO vollzieht im Vergleich zum bisher geltenden BDSG einen Paradigmenwechsel. Das BDSG stellt die rechtskonforme Datenverarbeitung in den Mittelpunkt. Die Bußgelder in Höhe bis zu 50.000 beziehungsweise 300.000 Euro adressieren deshalb ausgewählte Verstöße gegen das BDSG. Im Zentrum der DS-GVO steht dagegen die Befolgung ihrer gesamten Vorschriften. Beispiele für Verstöße, die ein Bußgeld auslösen können, sind:

» fehlende Dokumentation,
» unterlassene Wirksamkeitsprüfungen von Sicherheitsmaßnahmen,
» veraltete Betriebssystemversionen,
» Anbieten von Cloud-Services ohne angemessenes Sicherheitsniveau,
» fehlende Vertragsinhalte beim Einkauf von Cloud-Services oder
» nicht fristgerechte Meldung eines Sicherheitsvorfalls.

Der Bußgeldrahmen steigt auf bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Umsatzes des Vorjahres. Der höhere Wert ist maßgeblich. Die DS-GVO legt verschiedene Kriterien für die Ermäßigung des Bußgeldes fest, ohne jedoch die Höhe der Reduktion zu quantifizieren. Selbst eine 99-prozentige Reduktion der Bußgeldhöhe bedeutet immer noch eine Zahlung von 100.000 Euro. Auch diese Höhe ist für viele kleine und mittelständische Unternehmen existenzbedrohend. Auf ausgewählte Verstöße steht das „große" Bußgeld von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Umsatzes des Vorjahres. Auch hier ist der höhere Wert maßgeblich.

Darüber hinaus steht einer betroffenen Person, zum Beispiel einem Mitarbeiter oder Kunden, zukünftig Schadensersatz nicht nur für materielle, sondern auch für immaterielle Schäden zu. Angesichts der deutlich zunehmenden Risiken lohnt sich eine frühzeitige Beschäftigung mit der DS-GVO, um die Übergangszeit zu nutzen, die eigenen Systeme und Abläufe zu überprüfen und anzupassen.

Gesetzliche Vorgaben zur Sicherheitsorganisation

Auf den ersten Blick scheint die DS-GVO für die IT-Sicherheit wenig Neues zu fordern. Wie bisher richtet sich der Schutz auf personenbezogene Daten, wie zum Beispiel Name oder E-Mail-Adresse oder IP-Nummer (5). Daten ohne Personenbezug, beispielsweise Umsatzzahlen, Kostenkalkulationen oder Konstruktionspläne, sind formal nicht umfasst. In der Praxis lassen sich die beiden Arten kaum voneinander trennen, deshalb empfiehlt es sich, die gesetzlichen Vorgaben auch auf die nicht personenbezogenen Daten anzuwenden.

Die zukünftig geforderten Sicherheitskonzepte und Wirksamkeitsprüfungen finden sich schon länger auch in Normen und Standards (zum Beispiel BSI-Grundschutz, ISO

27001, DS-BvD-GDD-01 (6)). Im Unterschied zur bisherigen Regelung im BDSG (7) können zukünftig fehlende oder unzureichende Sicherheitsmaßnahmen mit einem Bußgeld von bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes belegt werden (8). Auch in den Details legt die DS-GVO neue Maßstäbe fest.

Sicherheitskonzeption

Sicherheit kann durch technische und auch durch organisatorische Maßnahmen erreicht werden. In der DS-GVO stehen beide Arten wie bisher gleichberechtigt nebeneinander. Die im Alltag anzutreffenden Sicherheitsstrategien liegen zwischen den gegensätzlichen Polen „analytische Konzeption" und „Virenscanner + Firewall reicht". Mit der DS-GVO legt der Gesetzgeber gerade für die „Virenscanner + Firewall reicht"-Fraktion die Latte deutlich höher. Unternehmen, die konzeptlos technische und organisatorische Maßnahmen aneinanderreihen, werden sich anstrengen müssen.

Zukünftig müssen die technischen und organisatorischen Maßnahmen der IT-Sicherheit den „Stand der Technik" berücksichtigen. Die Norm EN 45020 Normung – Allgemeine Begriffe (ISO/IEC Guide 2:2004) definiert in Ziffer 1.4 „Stand der Technik" wie folgt:

*„**Stand der Technik:** entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind, basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung."*

Der Stand der Technik ändert sich folglich, das heißt, Sicherheitsmaßnahmen müssen regelmäßig angepasst werden. Ein Blick auf das Betriebssystem Microsoft Windows zeigt die Problematik auf. Windows 10 ist die aktuelle Version, die sicherlich als Stand der Technik bezeichnet werden kann. Der Marktanteil im Januar 2016 lag bei 12,45 Prozent, während Windows 7, das im Oktober 2009 auf den Markt kam, auf 42,58 Prozent kommt (9). Entspricht Windows 7 noch dem Stand der Technik?

Die DS-GVO fordert nicht per se, die beste und teuerste Technik anzuschaffen. Sie verlangt „ein dem Risiko angemessenes Schutzniveau" zu etablieren. Schutzziele sind dabei (10):

- *„Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme auf Dauer sicherzustellen"* und
- die *„Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen".*

Weiterhin muss das Unternehmen durch geeignete Maßnahmen sicherstellen, dass die eingesetzten Personen personenbezogene Daten ausschließlich im Rahmen von Anweisungen und einschlägigen Gesetzen verarbeiten (11). Etablierte Maßnahmen sind unter anderem Berechtigungskonzepte auf Basis des „Need-to-know-Prinzips" und Tools zur Steuerung und Verwaltung von Berechtigungen. Für die Entscheidung für und gegen Maßnahmen verlangt die DS-GVO von Unternehmen, abzuwägen zwischen

- den Implementierungskosten,
- der Verarbeitungsart,
- dem Verarbeitungsumfang,
- den Umständen und den Zwecken der Verarbeitung sowie
- der Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten der von der Verarbeitung betroffenen Personen (Mitarbeiter, Nutzer, Kunden, Lieferanten usw.) (12).

Bei der Betrachtung der *„Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten"* sind sowohl die Konsequenzen aus der erwünschten Datenverarbeitung zu berücksichtigen wie auch die Risiken unzulässiger oder unerwünschter Vorkommnisse. Konkret müssen in der Abwägung insbesondere die Risiken folgender ungewollter Ereignisse berücksichtigt werden:

- Vernichtung,
- Verlust,
- Veränderung,
- unbefugte Weitergabe und
- unbefugter Zugang (13).

Die Beurteilung, wie viel Risiko akzeptabel ist, führt das Unternehmen durch. Die DS-GVO gibt für die Beurteilung keine Hilfestellung. Konkretisierungen können später durch aufsichtsbehördliche Entscheidungen, Gerichtsurteile und aufsichtsbehördlich anerkannte Standards die Beurteilung unterstützen. Explizit zu berücksichtigen ist, inwieweit Pseudonymisierung und Verschlüsselung sinnvoll eingesetzt werden können (14).

Da sich der Stand der Technik laufend ändert, neue Angriffsmethoden entwickelt und durch sich stetig erhöhende Rechenleistung Brute-Force-Angriffe immer leistungsfähiger werden, verändert sich die Abwägung ebenfalls. Eine periodische Überprüfung und Anpassung ist deshalb zwingend erforderlich (15).

Ein gutes Sicherheitskonzept leistet die geforderte Abwägung. Gleichzeitig fällt es mit einem Konzept leichter, nachzuweisen (16), dass angemessene Sicherheitsmaßnahmen eingesetzt werden, das heißt, faktisch wird das Erstellen und Aktuellhalten eines Sicherheitskonzepts Pflicht.

Wirksamkeitstest

Die Wirksamkeit von Sicherheitsmaßnahmen zu testen, gehört (theoretisch) zu den Selbstverständlichkeiten, die in der Praxis nicht durchgängig umgesetzt werden. Die DS-GVO spricht von einem *„Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit"* (17). Auch wenn der Wortlaut der DS-GVO lediglich fordert, dass dies *„gegebenenfalls"* umzusetzen ist, bleibt mit Blick auf den ebenfalls geforderten Stand der Technik festzuhalten, dass eine regelmäßige Überprüfung heute unter anderem in der ISO 27001 und im BSI-Grundschutz gefordert wird, das heißt Stand der Technik ist.

Ebenso wenig wird es genügen, lediglich einen Prozess zum Testen zu definieren, ohne die Tests auch tatsächlich durchzuführen. Empfehlenswert ist, die Testdurchführung und die Testergebnisse zu dokumentieren, um die Compliance mit der DS-GVO nachweisen zu können. Wie und in welchen Abständen Tests durchgeführt werden sollen, ist nicht geregelt. Hier kommen der Stand der Technik und die bereits aus dem Sicherheitskonzept bekannte Abwägung zum Tragen.

Die Pflicht, Wirksamkeitstests durchzuführen, ermächtigt nicht, im Rahmen von Wirksamkeitstests personenbezogene Daten zu verarbeiten. Es ist nach anderen Vorschriften der DS-GVO zu prüfen, ob die Verarbeitung

zulässig ist. Eine erlaubte Privatnutzung beispielsweise des PCs, der Unternehmens-E-Mail-Adresse oder des Internets stellen besondere Anforderungen an die Zulässigkeit, die im Einzelfall zu prüfen wäre.

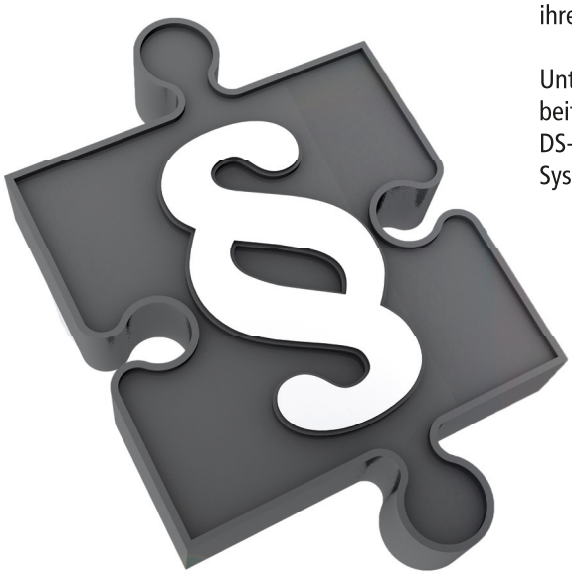
Melde- und Dokumentationspflichten bei Sicherheitsvorfällen

Wenn es zu einer Verletzung des Schutzes personenbezogener Daten kommt, kommen zusätzliche Dokumentations- und Meldepflichten auf das Unternehmen zu. Unter einer *„Verletzung des Schutzes personenbezogener Daten"*, im Folgenden verkürzt Sicherheitsvorfall genannt, versteht die DS-GVO eine Verletzung der Sicherheit, die zur Folge hat, dass personenbezogene Daten

- zufällig oder unrechtmäßig
  zerstört werden,
  verloren gehen,
  verändert werden oder
- unbefugt
  offenbart werden,
  Zugang gewährt wird,
  übermittelt werden,
  gespeichert werden oder
  anderweitig verarbeitet werden
  (18).

Erfasst sind damit grundsätzlich alle Spielarten der unbefugten Verarbeitung wie zum Beispiel Kenntnisnahme von Patientendaten wegen eines unversperrten Arzt-PCs, Abfrage der Kundendatenbank für private Zwecke durch Mitarbeiter oder das unbefugte Vernichten von Backup-Medien.

Eine zufällige Verletzung liegt beispielsweise bei einem Hardware- oder Softwarefehler vor. Die Verletzung erfolgt nicht absichtlich, sondern als Folge unzureichender Sicherungsmaßnahmen. Erfasst sind nur Vorfälle, die zu einem Datenverlust (zum Beispiel Festplattencrash ohne Backup) oder zu einer Datenveränderung (zum Beispiel irrtümliche Veränderung der Gehaltshöhe bei Überweisung) führen. Somit ist beispielsweise der vorübergehende Ausfall eines Servers kein Sicherheitsvorfall. Abgewehrte DDoS-Angriffe und vor der Aktivierung entfernte Schadsoftware stellen ebenfalls keine Sicherheitsvorfälle dar.



Grundsätzlich muss jeder Sicherheitsvorfall dokumentiert werden. Ab einer definierten Schwere ist zusätzlich die Datenschutzaufsichtsbehörde zu unterrichten. Bei besonders schwerwiegenden Vorfällen müssen zusätzlich alle betroffenen Personen informiert werden.

Dokumentation von Sicherheitsvorfällen

Jeder Sicherheitsvorfall muss dokumentiert werden, unabhängig davon, ob Meldepflichten ausgelöst werden (19). Die Dokumentation muss mindestens folgende Informationen enthalten:

- Beschreibung des Vorfalls,
- Beschreibung der Auswirkungen und
- Darstellung der Maßnahmen zur Behebung.

Die DS-GVO verlangt, dass die Dokumentation die Datenschutzaufsichtsbehörde in die Lage versetzen muss, prüfen zu können, ob die gesetzlichen Vorgaben zur Meldepflicht eingehalten wurden. Zu den Vorgaben zählt die Einhaltung der Reaktionsfrist und auch die Erläuterung, warum keine Meldepflicht ausgelöst worden ist. Da meldepflichtige Sicherheitsvorfälle innerhalb von 72 Stunden gemeldet werden müssen, empfiehlt es sich, Sicherheitsvorfälle unmittelbar nach ihrer Entdeckung zu dokumentieren.

Unternehmen, die Daten im Auftrag verarbeiten (heute § 11 BDSG und zukünftig § 26 DS-GVO), wie zum Beispiel Cloud-Anbieter, Systemhäuser und Rechenzentren, müssen jeden Sicherheitsvorfall unverzüglich an alle betroffenen Auftraggeber und nicht an die Datenschutzaufsichtsbehörde melden (20). Im Unterschied zur Meldepflicht gegenüber der Aufsichtsbehörde gibt es keine Ausnahmen. Der Auftraggeber ist für die Meldung gegenüber der Aufsichtsbehörde verantwortlich.

Meldepflicht gegenüber der Datenschutzaufsichtsbehörde

Meldepflichtig sind alle Unternehmen, sofern sie die betroffenen Daten nicht als Auftrags(daten)verarbeiter im Sinne von § 11 BDSG beziehungsweise Art. 26 DS-GVO verarbeiten. Auf eine Meldung des Sicherheitsvorfalls gegenüber der Datenschutzaufsichtsbehörde kann nur dann verzichtet werden, wenn dieser *„voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt"* (21). Zu den Risiken zählen jegliche physische, materiellen oder moralischen Schäden für die betroffenen Personen, wie zum Beispiel

- Verlust der Kontrolle über ihre Daten,
- Beschränkung ihrer Rechte,
- Diskriminierung,
- Identitätsdiebstahl,
- Betrug,
- finanzielle Schäden,
- unerlaubte Aufhebung von Pseudonymen,
- Verlust der Vertraulichkeit von Daten, die von einem Berufsgeheimnis geschützt werden und
- jeder andere wirtschaftliche oder soziale Nachteil (22).

Als Faustregel kann gelten, dass die Meldepflicht eintritt, sobald die betroffenen Personen voraussichtlich mit Nachteilen zu rechnen haben. Das Unternehmen muss die möglichen Folgen aus Sicht der Betroffenen analysieren und eine Prognose über die Folgen erstellen. Auf die Schwere der Folgen kommt es dabei nicht an. Es ist lediglich relevant, ob Folgen voraussichtlich eintreten können. Es liegt im Ermessen der Datenschutzaufsichtsbehörde, ob die Schwelle „voraussichtlich" im Einzelfall übersprungen wurde. Somit liegt die Schwelle für die Meldepflicht deutlich tiefer als heute (23).

Die Meldung hat *„ohne unangemessene Verzögerung und möglichst binnen höchstens 72 Stunden"* (24) nach Kennt-

nisnahme des Sicherheitsvorfalls zu erfolgen. Erfolgt die Meldung später als 72 Stunden nach Kenntnisnahme, muss die Verzögerung in der Meldung begründet werden. Die DS-GVO erlaubt explizit schrittweise Meldungen, das heißt die Informationen können im Zuge der Ermittlung nachgereicht werden. Die erste Meldung muss die 72-Stunden-Frist einhalten und auf die ausstehenden Informationen hinweisen. Die Meldung muss folgende Angaben umfassen (25):

- eine Beschreibung der Art der Verletzung,
- Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen (sofern möglich),
- Angabe der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze (sofern möglich),
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen für die Betroffenen,
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und
- wenn angemessen eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Eindämmung möglicher nachteiliger Auswirkungen für die Betroffenen.

Eine vollständige Meldung setzt eine Analyse des Sicherheitsvorfalls sowie das Planen von Gegenmaßnahmen voraus. Angesichts der kurzen Meldefrist empfiehlt es sich, einen Prozess zur Analyse und Meldung von Sicherheitsvorfällen zu etablieren.

Nicht nur eine unterlassene, unvollständige oder nicht fristgerechte Meldung kann ein Bußgeld nach sich ziehen. Auch unzureichende technische oder organisatorische Schutzmaßnahmen können zu einem Bußgeld führen. Maßnahmen zur Schadensbegrenzung für die Betroffenen, die vom Unternehmen ergriffen wurden, können sich bußgeldmindernd auswirken.

Information betroffener Personen

Zusätzlich zur Meldepflicht an die Datenschutzaufsichtsbehörde besteht eine Informationspflicht an die betroffenen Personen, wenn die Wahrscheinlichkeit besteht, dass der Sicherheitsvorfall ein hohes Risiko für deren persönliche Rechte und Freiheiten birgt (26). Die Schwellen sind das Bestehen einer Wahrscheinlichkeit und eines „hohen" Risikos. Wie hoch die Wahrscheinlichkeit oder das Risiko sein muss, ist in der DS-GVO nicht festgelegt. Dadurch steht dem Unternehmen ein Ermessensspielraum zu, der – fehlerhaft oder unzulässig – ausgenutzt auch zu einem Bußgeldrisiko führen kann. Umgekehrt wirkt sich eine „unnötige" Information der Betroffenen unter Umständen negativ auf die Reputation aus.

Die Information dient dem Zweck, es den Betroffenen zu ermöglichen, sich zu schützen (27). In den Erwägungsgründen wird davon ausgegangen, dass die Informationspflicht in enger Abstimmung mit der Datenschutzaufsichtsbehörde und den Strafverfolgungsbehörden erfolgen sollte (28). Vorgeschrieben ist die Abstimmung jedoch nicht. Gleichwohl kann die Datenschutzaufsichtsbehörde bei nicht erfolgter Information anordnen, dass die Information zu geben ist, oder auch selber die Betroffenen informieren. Sie kann auch per Beschluss feststellen, dass die Informationspflicht ausnahmsweise nicht besteht (29). Wenn eine der folgenden Voraussetzungen erfüllt ist, kann auf die Information verzichtet werden (30):

- Technische und organisatorische Maßnahmen machen die Daten für Unbefugte unverständlich (Verschlüsselung) oder
- nachträgliche Maßnahmen sorgen dafür, dass das hohe Risiko für die betroffenen Personen *„aller Wahrscheinlichkeit nach nicht mehr besteht"*.

Die DS-GVO schreibt kein Verschlüsselungsverfahren vor oder benennt Anforderungen an ein Verschlüsselungsverfahren. Ob ein Verschlüsselungsverfahren geeignet ist, bemisst sich nach dem Grad des Schutzes, den es vor unbefugter Kenntnisnahme bietet. Da es sich bei einem Verschlüsselungsverfahren um eine technische Maßnahme handelt, gilt wieder die Erfordernis „Stand der Technik" und die entsprechende Abwägung. Verfahren, die als gebrochen gelten oder die innerhalb eines überschaubaren Zeitraumes durch Brute-Force-Angriffe gebrochen werden können, dürften eher nicht

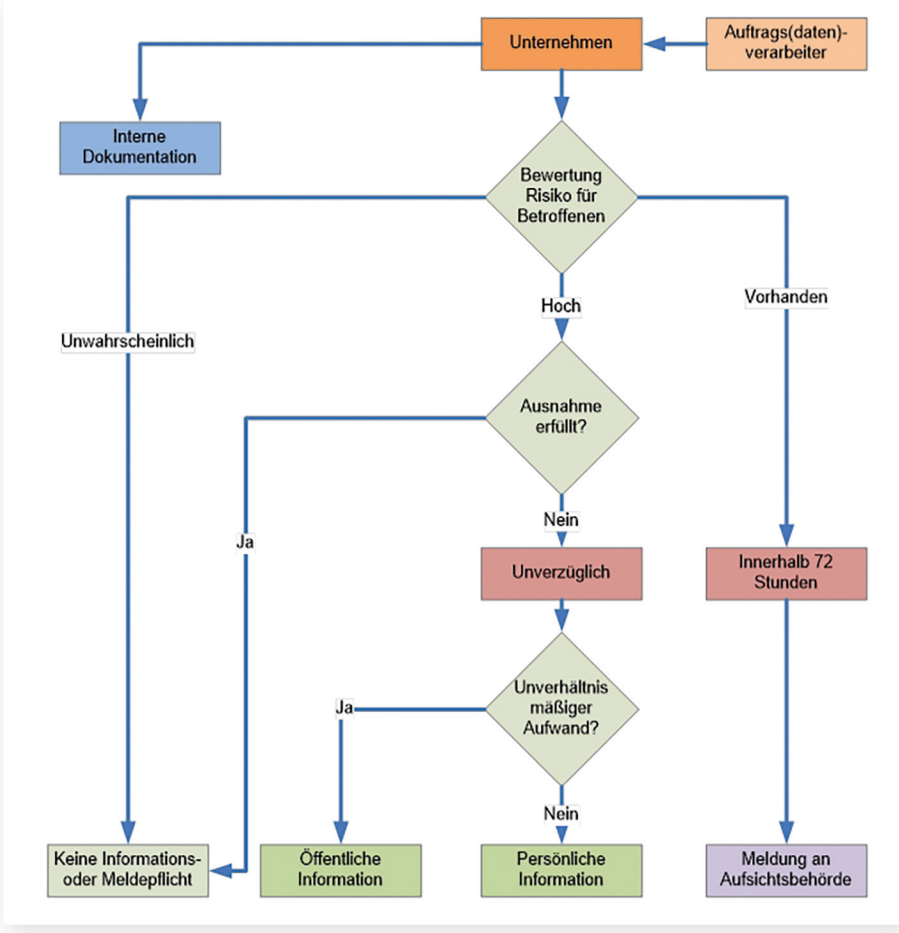


Bild 1: Entscheidungsbaum zur Melde- und Informationspflicht (34)

zum Entfallen des Risikos führen. Wesentlich dürfte auch sein, ob die Täter in den Besitz der Schlüssel gelangt sein könnten. (Siehe Bild 1).

Eine bekannte Maßnahme zur nachträglichen Risikoreduktion ist beispielsweise das Zurücksetzen von Passwörtern, nachdem diese unbefugt kopiert wurden. Bei der Beurteilung, ob durch das Zurücksetzen das hohe Risiko nicht mehr gegeben ist, sollte – neben anderen Aspekten – auch berücksichtigt werden, dass Verbraucher die gleichen Passwörter und Zugangsdaten gerne für mehrere Dienste verwenden. In einem solchen Fall wäre das Risiko weiterhin gegeben.

Wenn die Information der Betroffenen mit einem unverhältnismäßigen Aufwand verbunden ist, darf das Unternehmen statt der individuellen Information auch andere Maßnahmen ergreifen wie zum Beispiel eine öffentliche Bekanntmachung in Zeitungen. Diese Ersatzmaßnahme muss genauso wirksam sein wie eine individuelle Information (31). Eine Zeitungsanzeige in der Lokalzeitung wäre beispielsweise eher ungeeignet um deutschlandweit zu informieren. Wenn ausländische Personen betroffen sind, müssen diese ebenfalls informiert werden (32). Dabei ist zu beachten, dass die gewählte Sprache von den betroffenen Personen verstanden wird.

Die Information muss in einer für die Betroffenen verständlichen Sprache folgende Angaben umfassen (33):

- Beschreibung des Sicherheitsvorfalls,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen des Sicherheitsvorfalls,
- Beschreibung der wahrscheinlichen Folgen für die Betroffenen,
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und
- wenn angemessen eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Eindämmung möglicher nachteiligen Auswirkungen für die Betroffenen.

In Teil 2 behandeln wir die neuen Vorgaben bei der Auswahl von Produkten und deren Konfiguration, Zertifizierung und Standards und ziehen ein Fazit zur DS-GVO. ■

Quellenangaben und Erläuterungen

1.) *Jan Philipp Albrecht, Alles Wichtige zur Datenschutzreform, https://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html; zuletzt besucht am 24.02.2016.*
2.) *Offizielle Homepage: http://www.democracy-film.de/*
3.) *Rat der Europäischen Union, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN Die im Beitrag genannten Artikel aus der DS-GVO beziehen sich auf diese Fassung. Änderungen insbesondere in der Nummerierung können sich in der verabschiedeten Fassung ergeben.*
4.) *Müthlein, Thomas (2016): ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland. in: Recht der Datenverarbeitung, Nr. 2.*
5.) *Je nach Anwendungskontext lässt sich eine IP-Nummer einem Gerät, das ausschließlich von einem Anwender genutzt wird, zuordnen, bspw. bei einer statischen IP-Nummer oder innerhalb von Unternehmensnetzen.*
6.) *http://www.dsz-audit.de/wp-content/uploads/GDD-BvD-DATENSCHUTZSTANDARD-DS-BVD-GDD-01-V1-0.pdf*
7.) *§ 9 und Anlage BDSG*
8.) *Art. 79 Abs. 3 new Lit. a i:V.m. Art. 30 DS-GVO*
9.) *Statistica (2016): Marktanteile der führenden Betriebssystemversionen weltweit von Januar 2009 bis Januar 2016. URL: http://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/. Letzter Zugriff: 2016-03-02.*
10.) *Art. 30 Abs. 1 Lit. b, c DS-GVO*
11.) *Art. 30 Abs. 2b DS-GVO*
12.) *Art. 30 Abs. 1 DS-GVO*
13.) *Art. 30 Abs. 1a DS-GVO*
14.) *Art. 30 Abs. 1 Lit. a DS-GVO*
15.) *Art: 22 Abs. 1 und Art. 30 Abs. 1 Lit d DS-GVO*
16.) *Art. 5 Abs. 2 i.V.m. Abs. 1 DS-GVO*
17.) *Art. 30 Abs. 1 Lit. d DS-GVO*
18.) *Art. 4 Abs. 9 DS-GVO*
19.) *Art. 31 Abs. 4 DS-GVO*
20.) *Art. 31 Abs. 2 DS-GVO*
21.) *Art. 31 Abs. 1 DS-GVO*
22.) *Erwägungsgrund 67 DS-GVO*
23.) *Vgl. § 42a BDSG*
24.) *Art. 31 Abs. 1 DS-GVO*
25.) *Art. 31 Abs. 3 DS-GVO*
26.) *Art. 32 Abs. 1 DS-GVO*
27.) *Erwägungsgrund 67a new DS-GVO*
28.) *Erwägungsgrund 67a new DS-GVO*
29.) *Art. 32 Abs. 4 DS-GVO*
30.) *Art. 32 Abs. 3 Lit. b DS-GVO*
31.) *Art. 32 Abs. 3 Lit. c DS-GVO*
32.) *Art. 32 Abs. 1 DS-GVO grenzt die Informationspflicht weder territorial noch nach Herkunft der betroffenen Personen ein. Auch die Definition der betroffenen Personen in Art. 4 Abs. 1 DS-GVO kennt keine diesbezügliche Beschränkung. Der Zweck der DS-GVO, die Grundrechte gemäß der „Charta der Grundrechte der Europäischen Union" zu schützen, stützt diese Auslegung zusätzlich.*
33.) *Art. 32 Abs. 2 DS-GVO*
34.) *Quelle: Thomas Müthlein, mit geringfügigen Änderungen durch den Autor*

DR. NIELS LEPPERHOFF,
Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD e.V. und der GDD e.V.)