Bild: Shutterstock / kb-photodesign

Stichtag 25. Mai 2018

Der Countdown für die DSGVO läuft

So machen sich Unternehmen jetzt noch fit für die neue Datenschutz-Grundverordnung.

Im Frühjahr 2016 hat das Europäische Parlament die Datenschutz-Grundverordnung (DSGVO) auf den Weg gebracht. Betroffenen Unternehmen wurde zwei Jahre Zeit eingeräumt, um die neuen Regelungen umzusetzen. Ab dem 25. Mai 2018 ist die DSGVO beziehungsweise GDPR (General Data Protection Regulation), wie sie international genannt wird, in der Europäischen Union anzuwenden. Aber immer noch sind einige Firmen nur unzureichend auf die teils gravierenden Änderungen beim Datenschutz vorbereitet. Sie haben nicht nur Schwierigkeiten beim Auffinden und Klassifizieren der von ihnen gespeicherten Daten, nicht selten sind sie sich auch nicht darüber im Klaren, was sich zum Beispiel beim Umgang mit den eigenen Mitarbeitern ändert. Diese erhalten nämlich künftig erweiterte Rechte, um etwa zu erfahren, was ihr Arbeitgeber mit ihren Daten macht.

Unsicherheiten in Unternehmen

„Vielen ist nicht klar, worum es bei der Erfüllung der Anforderungen der DSGVO geht“, kommentiert Gerhard Unger, Regional Director DACH bei Bizagi. Das Unternehmen ist auf Software zur Automatisierung von Prozessen im Bereich Business Process Management (BPM) spezialisiert. Laut Unger geht es bei der Umsetzung der DSGVO im Kern um „digitalisierte und automatisierte Prozesse, die sicherstellen und dokumentieren, dass die Erhebung und Verarbeitung von Kundendaten in jedem Fall und ohne Ausnahme DSGVO-konform ablaufen“. Um dieses Ziel zu erfüllen, sind seiner Ansicht nach mehrere Artikel der DSGVO besonders relevant. So schreibe etwa der Abschnitt von Artikel 13 bis 15 vor, dass Unternehmen der Informationspflicht gegenüber ihren Kunden nachkommen müssen. Artikel 35 gebe vor, dass sie

„für jedes System, für jeden Server und für jede Anwendung die Verarbeitungstätigkeiten verzeichnen“ müssen. Das Ganze wird noch zusätzlich erschwert, weil sie laut Artikel 33 nur 72 Stunden Zeit haben, die zuständigen Aufsichtsbehörden „über eine Verletzung des Schutzes personenbezogener Daten zu informieren“.

Werden diese Vorgaben nicht erfüllt, dann drohen empfindliche Strafen. Beispielsweise können nach Aussage von Tim Wybitul, Fachanwalt für Arbeitsrecht in der Kanzlei Hogan Lovells in Frankfurt, bei Nichteinhaltung der Bestimmungen Bußgelder von bis zu 4 Prozent des weltweiten Jahresumsatzes erhoben werden. Aber auch „für Vorgesetzte, Datenschutzbeauftragte oder andere für den Umgang mit Informationen verantwortliche Entscheidungsträger drohen Geldbußen von bis zu 20 Millionen Euro“, schreibt Wybitul in einem Beitrag für die „Frankfurter Allgemeine Zeitung“. Dazu kämen eventuelle Schadenersatzforderungen sowie möglicherweise Kosten, die durch „immaterielle Schäden“ entstünden.

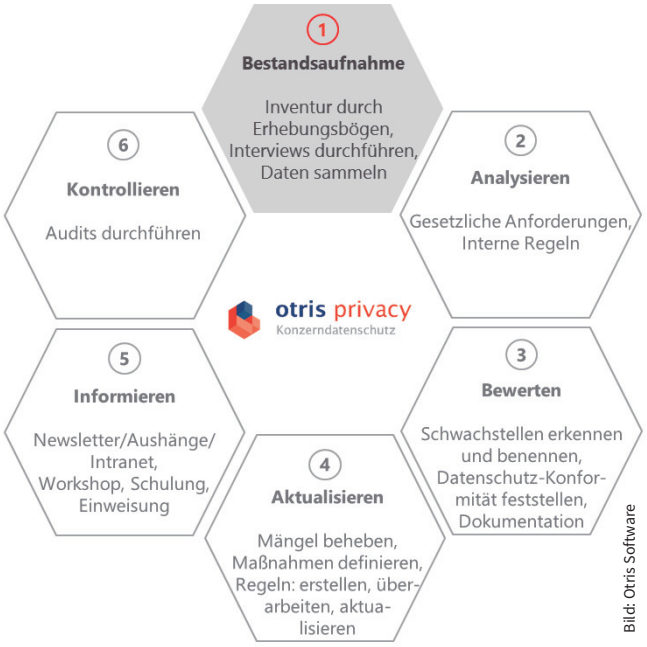

Bild: Otris Software

Datenschutz dokumentieren: Mit einer Spezial-Software wie Otris Privacy lässt sich ein Verzeichnis der Verarbeitungstätigkeiten erstellen.

Schwer kalkulierbare Kosten

Laut Anton Grashion, Senior Director Product Marketing EMEA beim Cyber-Security-Anbieter Cylance, gibt es „im Wesentlichen zwei Arten von Kosten, wenn es um die DSGVO geht: Zum einen die unumgänglichen Fixkosten und zum anderen die variablen Kosten“. Zu den Fixkosten gehören die Aufwendungen, die ein Unternehmen etwa für ein Audit seiner PII-Daten aufbringen muss. Die Abkürzung PII steht für Personally Identifiable Information beziehungsweise personenbezogene Daten. Zum Bereich der Fixkosten sind Grashion zufolge auch alle Arten von notwendig werdenden Assessments zu rechnen. Dazu zählen unter anderem der administrative und operationale Aufwand, der mit der Benennung und Etablierung eines Datenschutzbeauftragten verbunden ist, ebenso wie ein Berichtswesen, das sicherstellen soll, die individuellen Verbraucherrechtsanforderungen und Nachweispflichten zu gewährleisten. „Das sind Vorschriften, denen jede Firma Folge leisten muss“, so Grashion.

Bei den variablen Kosten sieht er dagegen eine regelrechte „Panikmache“. Bei ihnen handele es sich um diejenigen Aufwendungen, die entstehen können, wenn es zu einem sogenannten Datenschutzvorfall kommt, bei dem personenbezogene Daten betroffen sind. Als Beispiele für diese Art von Kosten nennt Grashion aber auch „Folgekosten durch entgangene Geschäfte, den entstandenen Rufschaden und natürlich die eigentlichen mit der Datenschutzverletzung assoziierten Strafen“. Regulierer und Regulierungsbehörden seien allerdings „sicherlich nicht dazu da, Firmen unnötig zu bestrafen, die Opfer einer Datenschutzverletzung geworden sind“.

Grashion ermahnt die Unternehmen aber nicht nur, alle nötigen Voraussetzungen für die DSGVO zu schaffen, sondern auch ihre Einhaltung zu überwachen. „Sie müssen die entsprechenden Berichte zur Verfügung stellen können“, betont der Cylance-Manager. Die Aufgabe der Regulierungsbehörden sei es, „den Forderungen der DSGVO Nachdruck zu verleihen“. Wie weit das dann konkret kontrolliert werden kann und wie weit es auch tatsächlich kontrolliert wird, sei aber noch unklar: „Wie sich das tatsächlich auswirkt, wenn die ersten Fälle in der Praxis auftreten, das ist eine ganz andere Sache.“ So genau weiß momentan also noch niemand, was nach dem Stichtag wirklich passiert.

Den IT-Abteilungen in Unternehmen rät Grashion: „Ganz platt gesprochen, verhindern Sie so weit als möglich, dass personenbezogene Daten von einer Datenschutzverletzung betroffen sind.“ Als Beispiel nennt er Bestimmungen der DSGVO, in denen es „um einige spezifische Reporting-Empfehlungen bei der Anzeigepflicht“ etwa von Ransomware gehe. Grashion weist darauf hin, dass es in Zukunft auch meldepflichtig sei, „wenn es einer Ransomware gelingt, personenbezogene Daten zu verschlüsseln“. Ebenso sei es meldepflichtig, wenn ein Unternehmen in diesem Fall „kein ausreichendes Backup gefahren“ habe.

Aber auch damit sei es noch nicht getan: „Selbst wenn Sie ein Backup haben, können die Regulierungsbehörden an dieser Stelle nachfassen“, so Grashion. Überprüft werde dann möglicherweise, „ob Sie ausreichende Datenschutzvorkehrungen getroffen haben, was insbesondere den Schutz vor Malware anbelangt“. Deswegen müssen eingesetzte Lösungen nachweislich einen ausreichenden Malware-Schutz bieten. ▶


Bild: Bizagi

„Vielen ist nicht klar, worum es bei der Erfüllung der Anforderungen der DSGVO geht.“

Gerhard Unger
Regional Director Bizagi DACH
www.bizagi.com/de

Kein Grund zur Panik

Zu Ruhe und Besonnenheit mahnt der Digitalverband Bitkom – selbst angesichts der langsam knapp werdenden Zeit. In einer Fragen- und Antwortsammlung zur Datenschutz-Grundverordnung weist Bitkom darauf hin, dass „viele der datenschutzrechtlichen Konzepte und Prinzipien der DSGVO im Großen und Ganzen nicht viel anders sind als auch bisher unter der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG)". Deren Vorschriften seien in Deutschland bereits mit dem Bundesdatenschutzgesetz (BDSG) umgesetzt worden. Wer sich also schon immer um das Thema Datenschutz gekümmert habe, der „sollte auch in Zukunft trotz der höheren Sanktionen nicht viel zu befürchten haben".

Was aber, wenn nicht? Dann sei es jetzt unumgänglich, die eigene Datenschutzpraxis zu überprüfen und das Datenschutzmanagement anzupassen und weiterzuentwickeln. Dabei gebe es keine Musterlösung, betont Bitkom: „Jedes Unternehmen führt durch sein eigenes Geschäftsmodell auch unterschiedliche Datenverarbeitungsvorgänge durch." Als Beispiele nennt er etwa den Anbieter einer Gesundheits-App, bei dem die Vorschriften für Gesundheitsdaten im Vordergrund stünden, wohingegen ein Cloud-Anbieter sich mit den neuen Haftungsregeln genauer auseinandersetzen müsse.

Checkliste zur DSGVO-Umsetzung

Anton Grashion, Senior Director Product Marketing EMEA bei Cylance, hat eine Checkliste erarbeitet, die Unternehmen bei der Umsetzung der Datenschutz-Grundverordnung helfen kann:

- Ein Audit für personenbezogene Daten im Unternehmen durchführen
- Detaillierte Aufzeichnungen im Hinblick auf die verarbeiteten Daten erstellen
- Alle Datenschutzhinweise überprüfen und aktualisieren
- Interne Richtlinien und die zugehörigen Prozesse überprüfen
- Privacy by Design und Privacy by Default implementieren
- Auch bei den Mitarbeitern muss das erforderliche Bewusstsein für die Umsetzung der DSGVO geschaffen werden
- Schulungen durchführen
- Interne Prozesse implementieren, um die Anzeigepflicht bei einem Datenschutzvorfall einzuhalten
- Planungen erstellen, was im Fall eines Datenschutzvorfalls zu geschehen hat und in welcher Reihenfolge
- Compliance-Verantwortlichkeiten personell festmachen und Budgets anweisen
- Einen Datenschutzbeauftragten benennen, schulen und in die Lage versetzen, dass er seinen Job den Anforderungen entsprechend erledigen kann

Bild: Cylance

„Die Regulierungsbehörden sind nicht dazu da, Firmen unnötig zu bestrafen, die Opfer einer Datenschutzverletzung geworden sind."

Anton Grashion
Senior Director Product Marketing EMEA bei Cylance
www.cylance.com

Mit der Verordnung werden zahlreiche neue Informations- und Dokumentationspflichten eingeführt, die von den Unternehmen umgesetzt werden müssen.

Völlig neu seien dabei gesetzliche Vorgaben wie die Berücksichtigung des Datenschutzes bei der Produktentwicklung (Privacy by Design) oder die Durchführung einer Datenschutzfolgenabschätzung. „IT-Unternehmen, die bis jetzt die Vorgaben der DSGVO ignoriert haben, sollten sich dringend überlegen, wie sie das Thema schnellstmöglich aufarbeiten können", drängt Susanne Dehmel, Geschäftsleiterin Vertrauen und Sicherheit bei Bitkom.

Zur Hilfestellung bei diesem Prozess hat der Digitalverband eine Reihe von Leitfäden zusammengestellt und veröffentlicht (www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/Inhaltsseite-2.html). Viele bislang geltende Regelungen wie etwa Betriebsvereinbarungen zum Datenschutz würden weiterhin gelten. Sie müssten allerdings in Zukunft zusätzlich die Vorgaben der DSGVO erfüllen. Überarbeitungen seien also unvermeidbar.

Nachweisbarkeit

Ein wichtiger Punkt bei der Umsetzung der neuen Datenschutz-Grundverordnung ist das Thema Nachweisbarkeit. Hier bieten sich Zertifizierungen nach IT-Grundschutz beziehungsweise ISO 27001 an. Unternehmen können mit einer Zertifizierung nachweisen, dass sie eine externe Firma geprüft hat.

Außerdem lernen sie dabei insbesondere auch das Thema Risikomanagement kennen. Das Wort Risiko tauchte im alten BDSG nicht einmal auf. Die DSGVO hat dagegen in Bezug auf alle organisatorisch-technischen Maßnahmen einen stärker risikobasierten Ansatz, der auch eine Dokumentation der Risikoeinschätzung nötig macht. Unternehmen müssen in Zukunft laut Bitkom deswegen „verschiedene Faktoren der Datenverarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigen". Und genau dies muss auch nachgewiesen werden können.

Für „besonders risikobehaftete Datenverarbeitungen" schreibt die DSGVO zudem die Durchführung einer Datenschutzfolgenabschätzung vor. Das gelte insbesondere dann, wenn es um automatisierte Entscheidungen geht, wenn zum Beispiel „massenhaft sensible Daten" verarbeitet oder wenn „systematisch öffentlich zugängliche Bereiche massenhaft beobachtet" werden sollen. Gegebenenfalls müssen dabei auch die Aufsichtsbehörden miteinbezogen werden. Tritt ein

„Risiko für die Rechte und Pflichten der Betroffenen“ ein, müssen diese und eventuell auch die Betroffenen informiert werden.

Pflicht: Verarbeitungsverzeichnis

Im Rahmen der erweiterten Dokumentationspflichten ist zudem künftig häufig ein „Verzeichnis der Verarbeitungstätigkeiten“ zu führen. Ausgenommen sind davon lediglich Unternehmen mit weniger als 250 Mitarbeitern, die laut Bitkom „nur in beschränktem Umfang und unkritische Daten verarbeiten“. Das Verarbeitungsverzeichnis sei nicht nur ein wichtiges Hilfsmittel für den Datenschutzbeauftragten, es könne auch als Nachweis gegenüber den Aufsichtsbehörden dienen. Die formale Verantwortlichkeit liege dabei bei der Unternehmensleitung. In der Praxis dürfte sich aber meist der Datenschutzbeauftragte, sofern es einen gibt, um dieses Thema kümmern. Die einzelnen Verfahrensmeldungen gehören dagegen wiederum zu den Aufgaben der Fachabteilungen.

Was fällt überhaupt unter die Verarbeitung von Daten? Bitkom hat dazu eine umfangreiche Liste erstellt: das Erheben, Erfassen, Ordnen, Auslesen, Abfragen, die Organisation, Speicherung, Anpassung oder Veränderung, Verwendung, Einschränkung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, das Löschen oder die Vernichtung von Daten.

Das Verzeichnis ist schriftlich zu führen, kann aber auch elektronisch mit einer Software für Textverarbeitung, Tabellenkalkulation, in einer Datenbank oder mit Hilfe von Spezialprogrammen erfolgen.

„Aus unserer täglichen Arbeit wissen wir, dass ein Global Player, der seine Datenschutzprozesse mit Word und Excel organisiert, keine Seltenheit ist“, kommentiert Christoph Niemann, Vorstand von Otris Software. Die neue Datenschutz-Grundverordnung komplett ohne Spezial-Software umzusetzen, werde vielen Firmen Schwierigkeiten bereiten, ist der Hersteller von Otris Privacy überzeugt. Dieses Programm soll die Einhaltung der geforderten Standards systematisch kontrollieren und analysieren sowie dabei helfen, die getroffenen Maßnahmen zu optimieren. So sollen sich nicht nur Sicherheitslücken erkennen und bewerten, sondern auch Datenschutzprozesse überwachen und dokumentieren lassen. Otris Privacy kann zudem Niemann zufolge dazu genutzt werden, eine Datenschutzfolgenabschätzung durchzuführen. ▶

Bild: Otris Software

„Aus unserer täglichen Arbeit wissen wir, dass ein Global Player, der seine Datenschutzprozesse mit Word und Excel organisiert, keine Seltenheit ist.“

Christoph Niemann
Vorstand von Otris Software
www.otris.de

DSGVO: Änderungen im Vergleich zum geltenden Recht

Der Digitalverband Bitkom hat zusammengestellt, was in der DSGVO anders geregelt ist als im BDSG.

- **Zweckänderung:** Der Grundsatz der Zweckbindung bleibt erhalten. Eine Weiterverarbeitung von personenbezogenen Daten ist nur bei „kompatiblen Zwecken“ zulässig und wenn sie „mit dem ursprünglichen Zweck vereinbar ist“.
- **Höhere Anforderungen an eine „informierte, freiwillige Einwilligung“:** Nicht mehr als Einwilligung gelten eine „angenommene stillschweigende Einwilligung“ durch den Kunden, Untätigkeit des Betroffenen oder etwa standardmäßig bereits angekreuzte Kästchen. Zudem ist ein Nachweis erforderlich, dass auch wirklich eine „effektive Einwilligung“ erteilt wurde.
- **Niedrigere Anforderungen an einen Widerruf der Einwilligung:** Auf der anderen Seite haben Betroffene das Recht, ihre Einwilligung „jederzeit“ und „ohne Begründung“ zurückzuziehen. Der Vorgang darf nicht aufwendiger sein als die Einwilligung.
- **Schärferes Koppelungsverbot:** Der Abschluss eines Vertrags darf nicht mit der Erteilung einer Einwilligung verbunden werden (kein „take it or leave it“).
- **Erweiterte Informations- und Auskunftspflichten:** Dazu gehören Angaben über die geplante Dauer der Speicherung personenbezogener Daten und Informationen zur Rechtslage.
- **Neue Portabilitätsverpflichtungen:** Daten, die Betroffene über sich angefordert haben, müssen in „gängigen Formaten“ wieder zur Verfügung gestellt werden. Auf Wunsch müssen sie auch an Dritte übermittelt werden.
- **Erweiterte Löschpflichten:** Unternehmen sollten dokumentieren können, welche personenbezogenen Daten verarbeitet werden und an wen sie weitergegeben wurden. Bei einem Löschanspruch durch Betroffene sollten die Daten außerdem schnell aufgefunden und gelöscht werden können.
- **Erweitertes Widerspruchsrecht:** Betroffene können künftig „Datenverarbeitungen zu Zwecken des Direktmarketings“ widersprechen, das gilt auch für die Bildung von Nutzerprofilen.
- **Geänderte Pflichten in Auftragsverhältnissen:** Nicht mehr nur der für eine Verarbeitung Verantwortliche haftet für eine Datenpanne, sondern auch der „Auftragsverarbeiter“. In diesem Bereich tätige Unternehmen müssen künftig „eine schriftliche beziehungsweise elektronische Dokumentation ihrer Verarbeitungstätigkeiten führen und auf Verlangen der Aufsichtsbehörde zur Verfügung stellen“.

Ist die Frage der Umsetzung geklärt, geht es um die konkrete Erstellung eines Verarbeitungsverzeichnisses. Bitkom schlägt dafür diese Schritte vor:

- **Sensibilisierungsphase:** In diesem Schritt sollten die Fachbereiche über die gesetzlichen Vorgaben und die Zielsetzung in Kenntnis gesetzt werden, zum Beispiel durch Mailings oder Artikel im Intranet.
- **Informationsphase:** Mitarbeiter, die einbezogen werden sollen, werden mit dem Vorhaben vertraut gemacht, etwa durch Workshops und die gemeinsame Bearbeitung eines Musterfalls.
- **Abfragephase:** Vorbereitete Fragebögen werden zur Erfassung der bestehenden Verarbeitungen von personenbezogenen Daten mit einem Rückgabetermin an die Fachbereiche versendet.
- **Beratungsphase:** Diese Phase steht für Rückfragen zur Verfügung. Dabei ist zum Beispiel die Einrichtung einer Hotline hilfreich.
- **Konsolidierungsphase:** Die vorgelegten Verfahrensmeldungen werden konsolidiert, um das Verarbeitungsverzeichnis „übersichtlich und handhabbar" zu halten.
- **Umsetzungsphase:** Nachdem sichergestellt werden kann, dass alle abgegebenen und gesammelten Informationen vollständig und richtig sind, werden sie im Verarbeitungsverzeichnis erfasst.
- **Pflegephase:** In manchen Fällen ist es ratsam, etwa eine interne Revisionsabteilung zu beauftragen, im Rahmen ihrer Routineprüfungen auch die Aktualität der Verfahrensmeldungen zu kontrollieren.

Anhand dieser Zusammenstellung wird klar, dass es sich dabei um einen relativ aufwendigen Prozess handelt, der bis zum Stichtag im Mai kaum noch zu schaffen sein dürfte. Allerdings geht es deutlich schneller, wenn in einem Unternehmen bereits vollständige Aufstellungen aller Verarbeitungsvorgänge vorliegen, die auch zur Umsetzung der DSGVO genutzt werden können. In vielen Fällen ist es zudem empfehlenswert, sich die Hilfe externer Berater zu holen oder zumindest spezialisierte Lösungen einzusetzen, die den Vorgang beschleunigen können.

Lösungen für die DSGVO

Welche Möglichkeiten haben Unternehmen, die verbliebene Zeit zu nutzen, um sich besser auf die DSGVO vorzubereiten? Gerhard Unger von Bizagi empfiehlt einen ganzheitlichen Ansatz, der „aus einer technischen Plattform zur Definition digitalisierter und automatischer Prozesse, einer Implementierung dieser Prozesse in die IT-Infrastruktur sowie einem kontinuierlichen Qualitätsmanagement und der Zertifizierung dieser Prozesse besteht". Unger ist überzeugt, dass sich dann auch „einfacher ein interner oder externer Datenschutzbeauftragter findet, der die rechtliche Verantwortung für die Datenverarbeitung übernimmt".

Bild: Thales eSecurity

„Die DSGVO ist eine große Chance, den Datenschutz als Wettbewerbsvorteil zu erkennen und ihn nicht nur als Kostenfaktor oder Innovationshemmnis zu betrachten."

Kai Zobel
Regional Director bei
Thales eSecurity
http://de.thalesesecurity.com

Christophe Bertrand, Vice President Product Marketing beim Datensicherungsspezialisten Arcserve, erinnert daran, dass die DSGVO jedem EU-Bürger das Recht gibt, seine Einwilligung in die Erhebung persönlicher Daten zurückzuziehen. Das schließe auch die endgültige Löschung seiner E-Mails und anderer personenbezogener Informationen ein. Das Recht zum Löschen personenbezogener Informationen sei dabei jedoch nur ein Aspekt. Bertrand: „Es geht explizit auch um den Schutz dieser Daten, der wiederum operative Entscheidungen bei der Datensicherung und Wiederherstellung bedingt."

Bild: Arcserve

„Die Datenschutz-Grundverordnung gibt jedem EU-Bürger das Recht, seine Einwilligung in die Erhebung persönlicher Daten zurückzuziehen."

Christophe Bertrand
Vice President Product
Marketing bei Arcserve
www.arcserve.com/de

Er empfiehlt daher „leistungsfähige und einfach zu bedienende Lösungen, die das rasche Identifizieren und Löschen personenbezogener Daten in den unternehmenseigenen Systemen ermöglichen". Dazu gehören ihm zufolge zum Beispiel „die Datensicherung und Wiederherstellung aus einer einheitlichen Konsole, die granulare Wiederherstellbarkeit von Daten mit der Möglichkeit, spezifische Daten auszuschließen, sowie ein vollständiges Reporting aller Aktivitäten". Für essenziell hält er zudem Funktionen, mit denen ein Administrator etwa „umgehend persönliche E-Mails identifizieren und löschen" kann, wenn ein Kunde seine Einwilligung in die Datenerhebung zurückzieht. So ließen sich die DSGVO-Konformität garantieren und Sanktionen vermeiden.

Fazit

Die Frist zur Umsetzung der DSGVO läuft ab. Kai Zobel, Regional Director beim Anbieter von Datensicherheitslösungen Thales eSecurity, rechnet damit, dass „tatsächlich verschiedene juristische Probleme auf Unternehmen zukommen und die Öffentlichkeit über Datenschutzverletzungen eher Bescheid weiß als jemals zuvor". Es bleibe allerdings abzuwarten, ob die Bedenken bezüglich der Auswirkungen der DSGVO auf Geschäftsprozesse, Innovationen und internationale Beziehungen berechtigt sind. Wie andere Experten auch, sieht Zobel die DSGVO vielmehr als „große Chance, den Datenschutz als Wettbewerbsvorteil zu erkennen und ihn nicht nur als Kostenfaktor oder Innovationshemmnis zu betrachten". ■

Andreas Th. Fischer/kpf
kpf@com-professional.de