storage-magazin.de

Ausgabe **2-2018**

Eine Publikation von **speicherguide.de**

Grafik: fotolia.de / istockphoto.com / speicherguide.de

Recht

Dokumentation

Datenschutz

DSGVO

Kontrolle

Datensicherheit

Prozesse

Datensicherheit

Verschlüsselung

Technologie

Überwachung

Privatsphäre

Unternehmen

IT

Sicherheit

Daten

DSGVO: Sehen Sie die Chance – hilft ja nix …

Karl Fröhlich, Chefredakteur speicherguide.de

Liebe Leserinnen und Leser,

die DSGVO ist vermutlich auch bei Ihnen in der Firma ein Reizthema, oder? Kaum einer hat Spaß daran. Die Unternehmensverantwortlichen sehen die Verordnung als Gängelung und größtenteils als unnütze Geldausgabe. Verübeln kann man diese Sichtweise keinem, zu unausgegoren und unklar sind die Forderungen. Selbst als Verbraucher habe ich nicht den Eindruck, dass meine Daten nun besser geschützt sind.

Im Prinzip wollte die EU den großen Konzernen und Social-Media-Plattformen Grenzen aufzeigen, im Umgang mit personenbezogenen Daten. Das Gegenteil ist eingetreten. Die Großen gehen die DSGVO eher gelassen an und Facebook & Co zeigen vielmehr den Behörden ihre Grenzen auf. Wortreich wurde den Anwendern etwas von Datenschutz und der Sicherheit ihrer Daten erklärt. Wer die Plattformen weiter nutzen möchte, muss die Checkbox bestätigen und damit in alles einwilligen. Einschränkungen auf Unternehmensseite sind dabei nicht vorgesehen.

Zurück bleibt einmal mehr der fade Beigeschmack, die da oben dürfen alles, wir da unten, können schauen wo wir bleiben. Was sich vermutlich auch manche IT-Abteilung denkt … Die DSGVO gilt uneingeschränkt für alle Gewerbetreibenden. Hinzukommt eine mehr als schlechte Öffentlichkeitsarbeit der Aufsichtsbehörden. Anstelle die Chancen und Möglichkeiten der Verordnung in den Vordergrund zu stellen, überließ man die Kommunikation vor allem Anwälten und selbsternannten Experten. Das Ergebnis: Zum Stichtag am 25. Mai wusste eine nicht zu verachtende Zahl an Unternehmensvertretern nichts oder nur ungenügend über die DSGVO Bescheid. Und die, die schon davon gehört hatten, denken vor allem, die DSGVO ist böse, kostet Geld und wenn‘s blöd läuft drohen hohe Strafen. Da ist als Außenstehender schon die Frage gestattet, »geht das nicht besser?«.

Der Datenschutz war bei uns auf speicherguide.de schon immer ein Thema. Im Vorfeld der DSGVO kamen da natürlich einige Artikel hinzu und nachdem ich mich zum Datenschutz-Yogi weitergebildet habe, sind meine Datenschutz-Kolumnen nun fester Bestandteil unserer redaktionellen Berichterstattung. In diesem Special arbeiten wir die Anforderungen der DSGVO im Unternehmen nochmal auf und schauen auch, was dies für den IT-Betrieb bedeutet. Sehen Sie die DSGVO als Chance, hilft ja nix...

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Inhalt

Datenschutz betrifft alle Gewerbetreibenden und das gesamte Unternehmen

DSGVO im Unternehmen

In der Praxis sehen Firmen die DSGVO vor allem als lästiges Übel. Die neue Datenschutzregelung ist für Unternehmen aber auch die Chance, eine seriöse Informationspolitik und zeitgemäße Sicherheitsmaßnahmen zu etablieren. Wichtig: Betroffen sind alle Gewerbetreibenden und die gesamte Firma und die Verantwortlichen – meist die Geschäftsleitung – haften für etwaige Verstöße.

Karl Fröhlich

Nie stand der Datenschutz so im Fokus wie in diesem Jahr. Zu verdanken haben wir dies der neuen »EU-Datenschutz-Grundverordnung« (EU-DSGVO), die alle Unternehmen in Europa seit dem 25. Mai 2018 umgesetzt haben sollten. In der Theorie waren zwei Jahre dafür Zeit. Im ersten Jahr war aber in Deutschland kaum etwas dazu bekannt, wie die DSGVO hätte umgesetzt werden sollen. Daher blieb den Datenschützern eigentlich nur ein Jahr. Hinzukommt, dass viele Firmen viel zu spät angefangen haben. Höflich gesagt, sehr viele haben es unterschätzt – man könnte auch ignoriert sagen.

In einer *speicherguide.de*-Umfrage im Oktober 2017, sahen sich knapp die Hälfte der Befragten im Plan bzw. hielten es für möglich, bis zum 25. Mai noch das geforderte Soll zu erreichen. Ungefähr im gleichen Zeitraum erklärt **IDC**, dass 44 Prozent einer IDC-Studie noch keine konkreten technologischen oder organisatorischen Maßnahmen zur Vorbereitung auf die DSGVO getroffen hätten. Bis zum Stichtag dürften noch einige Vollzugsmeldungen hinzugekommen sein. Aus Gesprächen mit Datenschutzexperten und auch unserer eigenen Erfahrung zufolge, dürfte mindestens ein Drittel der kleinen und mittleren Unternehmen (KMUs) bezüglich der DSGVO nicht compliant gewesen sein.

Bei kleinen Betrieben sieht es noch drastischer aus: »Vor allem Unternehmen unter 20 Mitarbeitern hatten den Stichtag 25. Mai unterschätzt – obwohl es bereits eine Übergangszeit für zwei Jahren gegeben hatte«, erklärt Datenschutzexperte **René Rautenberg** von **ER Secure**, Hersteller eines Datenschutz-Managementsystems. »Darüber hinaus ist vielen Unternehmen erst im April/Mai bewusst geworden, dass es bei der Verordnung um mehr als die Double-Opt-In-Regel bei Werbemails geht, die ohnehin im Wettbewerbsrecht geregelt ist und jetzt lediglich verschärft wurde.«

Die DSGVO betrifft alle Gewerbetreibenden

Pauschal gilt, die DSGVO betrifft jeden Gewerbetreibenden. Es ist nahezu ausge-

schlossen, dass man in Deutschland unternehmerisch tätig sein kann, ohne in irgendeiner Form personenbezogene Daten zu verarbeiten. Das **Bayerische Landesamt für Datenschutzaufsicht** stellt in seiner Broschüre mit dem Titel: »Erste Hilfe zu Datenschutz-Grundverordnung für Unternehmen und Vereine – ein Sofortmaßnahmenpaket« drei einfache Fragen:

- Biete ich Dienstleistungen oder Waren in Deutschland an?
- Biete ich Dienstleistungen oder Waren in der EU an?
- Habe ich Mitarbeiter in meiner Firma?

Wenn man auch nur **eine Frage mit »ja« beantworten kann, ist die DSGVO anwendbar** und demnach auch verpflichtend.

DSGVO betrifft das komplette Unternehmen

Wichtig ist zu erkennen, dass die DSGVO das gesamte Unternehmen betrifft und nicht nur die Webseite und den Newsletter. »Der Datenschutz muss in allen Abteilungen angewandt werden und bezieht sich nicht nur auf Kundendaten«, mahnt die Münchener Datenschutzexpertin **Sabine Noack**. »Die DSGVO schließt auch die Daten der Mitarbeiter (Voll- und Teilzeit), von Lieferanten, Partnern und Dienstleistern mit ein.«

Der Datenschutz beginnt aber außerhalb der IT: Die technischen und organisatorischen Maßnahmen (TOM) zur Datensicherheit schließen auch eine Zutritts-, Zugangs- und Weitergabekontrolle mit ein. »Das heißt, es dürfen nur Befugte Zutritt zu den Geschäftsräumen haben«, sagt **Frederik Freckmann**, externer Datenschutzbeauftragter aus Berlin. »Das ist natürlich nicht neu, im Rahmen der TOM müssen aber der Zutrittsprozess, die Befugnis und die Zuständigkeit sauber dokumentiert werden.« Dies gelte auch für die Weitergabe von Datenträgern, schließt mobiles Arbeiten mit ein und geht bis zu einer Regelung, was mit alten Datenträgern passiert.

Für alle die zur Zutrittskontrolle ein Chipkartensystem nutzen: »Auch diese sind datenschutzrelevant, weil sie auslesbar sind – woraus sich Rückschlüsse auf Mitarbeiter und ihr Verhalten ziehen lassen«, ergänzt Datenschutzexperte Rautenberg. »Wir unterstützen hier mit einem Fragebogen, der den Prozess durchleuchtet und mit dem Unternehmen ihre Situation individuell dokumentieren können.«

Dokumentationspflicht erfüllen

Die DSGVO zwingt Unternehmen, sich sämtliche Abteilungen und Prozesse neu vorzunehmen. »Abhängig von Geschäftsfeld, Größe und Branche sollten bei KMUs alleine für die Dokumentation der Verarbeitungstätigkeiten mindestens drei Personentage angesetzt werden«, erklärt Datenschutzexperte **Frank Giebel** von **3rd Mind Business Consulting**. »Wichtig ist, dass der Datenschutz als Chefsache gesehen wird. Geschäftsleitung und Vorstandsebene müssen den Datenschutz ernst nehmen. Dies ist zwar bereits seit der letzten BDSG-Novelle in 2009 so, richtig ›angekommen‹ scheint es bei manchen aber erst mit der DSGVO zu sein. Diese nimmt die ›Verantwortlichen‹ auch persönlich in die Haftung und unterwirft diese einer Nachweis- und Rechenschaftspflicht, die Vorgaben eingehalten zu haben. Mit Blick auf die exorbitant erhöhten möglichen Bußgelder und weiteren Sanktionen ist klar, dass es der EU

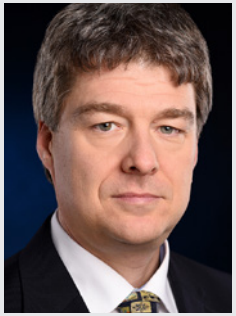


Foto: ER Secure

René Rautenberg
ER Secure

»Firmen sollten ihre Mitarbeiter für den Datenschutz sensibilisieren. Vielen ist überhaupt nicht bewusst, dass sich Unbefugte durch zwischenmenschliche Beeinflussung Zutritt in Büroräume verschaffen.«

Foto: Sabine Noack

Sabine Noack
Datenschutzbeauftragte

»Die DSGVO bezieht sich nicht nur auf Kunden, sondern schließt auch die Daten der Mitarbeiter (Voll- und Teilzeit), von Lieferanten, Partnern und Dienstleistern mit ein.«

Foto: Frank Giebel

Frank Giebel
3rd Mind Business Consulting

»Geschäftsleitung und Vorstandsebene müssen den Datenschutz ernst nehmen. Die DSGVO unterwirft die Verantwortlichen einer Nachweis- und Rechenschaftspflicht.«

Fragenkatalog zu technischen und organisatorischen Maßnahmen zur Datensicherheit

Die getroffenen Maßnahmen sind möglichst konkret zu beschreiben. Die reine Angabe von Stichworten reicht nicht aus. Seien Sie hier möglichst genau.

Sollte es in Einzelfällen keine abschließenden Maßnahmen geben, zum Beispiel weil man sich komplett dagegen entschieden hat oder die Evaluierung und Einführung noch andauert, begründen Sie auch dies möglichst ausführlich.

1. Vertraulichkeit

Zutrittskontrolle

Hier geht es darum, wie die Gebäude oder Büroräume, in denen Daten verarbeitet werden, vor dem unberechtigten Zutritt geschützt sind. Dazu gehört unter anderem, ob es eine Besucherregelung gibt, ein Zutrittskonzept vorhanden ist oder eine Videoüberwachung bzw. Alarmanlage genutzt wird.

Zugangskontrolle

Hier wird erörtert, wer Berechtigungen zum Zugang zu Daten oder Systemen erteilt. Dazu gehört unter anderem, ob diese protokolliert werden und wer die Berechtigungen überwacht, ob es im Unternehmen Passwortrichtlinien gibt, externe Schnittstellen (USB) gesperrt sind und ob mobile IT-Systeme und Datenträger verschlüsselt werden. Auch ist hier festzuhalten, wie IT-Systeme vor Viren und Schad-Software geschützt werden und ob das System unberechtigte Zugriffe von Dritten erkennt und unterbindet.

Zugriffskontrolle

Die Zugriffskontrolle dokumentiert beispielsweise wie sichergestellt wird, dass Benutzerrollen und damit einhergehende Berechtigungen differenziert vergeben werden. Zudem gilt es zu regeln, dass nicht mehr verwendete Datenträger sicher gelöscht oder vernichtet und Papierunterlagen mit personenbezogenen Daten sicher vernichtet werden und wie das Unternehmen die Vernichtung nachweisen kann.

Trennung

Es gilt sicherzustellen, dass Daten, die zu verschiedenen Zwecken verarbeitet werden, getrennt voneinander verarbeitet werden.

Pseudonymisierung & Verschlüsselung

Personenbezogene Daten sollten nach Möglichkeit pseudonymisiert werden, mit einem nicht personenbezogenen Namen, einer Nummer oder ähnlichem. Wie alle anderen TOM ist dies nicht verpflichtend. Eine Verschlüsselung unterstützt vor unberechtigten Zugriff. Wann und wie kommt eine Verschlüsselung zum Einsatz?

2. Integrität

Eingabekontrolle

Weitergabekontrolle

3. Verfügbarkeit und Belastbarkeit

Für diesen Fragenbereich benötigen Sie Ihre IT-Abteilung. Hier soll der Sicherheitsstand der IT dokumentiert werden, von der USV bis zum Notfallplan.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Hier ist vor allem Ihr Datenschutzbeauftragter gefragt sowie diejenigen, die die Verantwortung für Datenschutz und Informationssicherheit übernommen haben. Es gilt zu dokumentieren, welche Maßnahmen zur Einhaltung der DSGVO unternommen wurden, wie und wer diese überprüft, welche Leit- und Richtlinien eingeführt wurden.

Mit der TOM-Dokumentation belegen Sie im Bedarfsfall, dass Sie alles Nötige bedacht haben, um die personenbezogenen Daten zu schützen, die in Ihrem Unternehmen verarbeitet werden. Auf Verlangen sind sie der für Sie zuständigen Aufsichtsbehörde vorzulegen.

Es kann aber auch sein, dass Geschäftspartner Einsicht in Ihre TOM verlangen. Dazu sind Sie nicht verpflichtet. Es könnte Ihrem Unternehmen aber einen Auftrag kosten. Anders herum können auch Sie sich bei Ihren Lieferanten oder Dienstleistern rückversichern, dass diese auch beim Datenschutz ihrer Sorgfaltspflicht nachkommen.

Eine Mustervorlage des TOM-Fragebogen erhalten Sie über unseren Chefredakteur und zertifizierten Datenschutzbeauftragten, Karl Fröhlich (kfroehlich@speicherguide.de).

Quelle: datenschutz-guru.de/Datenschutz Fröhlich

sehr ernst damit ist; ein ›weiter so‹ oder die Ansicht, ›Datenschutz ist nur ein notwendiges Übel‹ ist daher nicht nur veraltet, sondern mittlerweile nach vorgenanntem sehr gefährlich.«

Der zu erbringende Aufwand hängt natürlich von der Unternehmensgröße, der Branche und Komplexität des Geschäftsfeldes ab. Wobei sich schon sagen lässt, für kleine Betriebe ist der Aufwand meist durchaus überschaubar. Datenschutzexperten raten dazu, sämtliche Bereiche schrittweise an das neue Regelwerk anzupassen, in denen Daten von Mitarbeitern, Kunden und Lieferanten erfasst und verarbeitet werden. »Rund 80 Prozent der Unternehmen können die schärferen Datenschutzregeln mit Hilfe einer entsprechenden Software bzw. externen Datenschutzbeauftragten selbst realisieren«, meint Rautenberg. Er warnt Unternehmen aber auch davor, sich in trügerischer Sicherheit zu wähnen: »Im Augenblick haben die Behörden selbst alle Hände voll zu tun. In Bayern etwa wurde die Frist für alle Unternehmen ab dem zehnten Mitarbeiter bis 30. September 2018 verlängert, einen Datenschutzbeauftragten zu ernennen und zu melden. Diesen Aufschub sollten Unternehmen nutzen und ihre Hausaufgaben machen. Wer nachweisen kann, dass er das Thema ernst genommen hat, hat im Ernstfall bessere Karten.«

DSGVO: Unternehmen sollten die Chance nutzen

Firmen sollten aber nicht nur den Aufwand sehen. »Die DSGVO ist wichtig«, mahnt die Münchener Expertin Noack. »Weil der Schutz der personenbezogenen Daten von Mitarbeitern, Kunden und Interessenten in Zeiten von ungezügeltem Profiling und damit einhergehenden Missbrauchsmöglichkeiten endlich die Priorität bekommen hat, die er verdient.

Unternehmen können die DSGVO als Anlass nehmen, Prozesse, in denen personenbezogene Daten verarbeitet werden, nicht nur datenschutzkonform zu gestalten, sondern auch den einen oder anderen alten Zopf abzuschneiden, Unnötiges los zu werden, längst überfällige Sicherheitsmaßnahmen zu etablieren und mit einer seriösen Informationspolitik bei Kunden, Partnern und Interessenten zu punkten.«

»Unternehmen sollten den Anlass nutzen, um Mitarbeiter auch für dieses Thema zu sensibilisieren«, ergänzt Rautenberg. Vielen sei beispielsweise nicht bewusst, dass es Methoden wie Social-Engineering gebe, bei denen sich Unbefugte durch zwischenmenschliche Beeinflussung Zutritt in Büroräume verschaffen, indem sie sich etwa geschickt nach einem Mitarbeiter erkundigen oder einen anderen glaubwürdigen Vorwand angeben. ■

Die IT muss die Bürokratie des Datenschutzes lösen

DSGVO im IT-Betrieb

Ein effizienter Schutz personenbezogener Daten ist ohne Informationstechnologie nicht realisierbar. Man könnte auch sagen, die IT muss die von der DSGVO ausgelöste Bürokratie nun lösen. Die Umstellung der IT-Systeme ist für Unternehmen dabei eine große Herausforderung.

Karl Fröhlich

Mit der DSGVO kommt der Datenschutz im Zeitalter von Cloud-Computing und Big-Data an. Für Unternehmen hat das zunächst sehr viel mit Organisation und Recht zu tun, aber auch mit Prozessen und Technologie. Daher ist die DSGVO auch ein IT-Thema, ein sehr großes sogar.

Vieles ist nicht neu, wie zum Beispiel die Zugriffskontrolle. Es ist ganz selbstverständlich, dass nicht jeder auf sensible Daten zugreifen darf. Im Falle von personenbezogenen Daten muss nun allerdings dokumentiert werden, wo diese wie gespeichert sind und wie sichergestellt wird, dass nur berechtigte Personen darauf zugreifen können. Klingt erstmals simple, doch wie sich zeigt, besitzen nur wenige eine durchgängige Dokumentation und so dürfen IT-Beauftragte zum Teil lange Gespräche mit den Datenschutzbeauftragten führen.

Dokumentation und Reporting

Die Dokumentation und auch ein Reporting zieht sich wie ein roter Faden durch die IT-seitige Umsetzung der DSGVO. Einerseits gilt es festzustellen, wo personenbezogene Daten im Unternehmen verarbeitet und gespeichert werden. Andererseits müssen Firmen ein Verfahren entwickeln und dokumentieren, wie man künftig mit diesen Daten umgehen will. Zunächst müssen diese Daten aber identifiziert, klassifiziert und indexiert werden. Ziel ist es einen möglichst automatischen Prozess zu etablieren.

Erschwerend kommt hinzu, dass Firmen die erhobenen Daten nur für den ursprünglichen Zweck verarbeiteten dürfen (Art. 5 Abs. 1 lit. b DSGVO). Auch wenn es praktisch und einfach wäre, wer die Daten für ein neues Projekt nutzen möchte, benötigt dafür eine vorherige Einwilligung. Werden die personenbezogenen Daten für den ursprünglichen Zweck nicht mehr benötigt, muss das Unternehmen diese Daten löschen – sofern keine rechtlichen Gründe dagegensprechen.

Die Krux mit der Löschpflicht

Auch das Löschen ist eine Pflicht: Betroffene Personen können eine zuvor abgegebene Einwilligung widerrufen oder Widerspruch gegen die weitere Verarbeitung ihrer Daten einlegen und die Löschung beantragen. Hier spielt auch die Auskunftspflicht mit hinein.

In Datenschutzkreisen werden dies Leute gerne als Unruhestifter bezeichnet. So lästig diese Gesuche auch sind, desto ernster sollten Unternehmen sie nehmen. Diese Personen haben sich meist intensiv mit der Thematik auseinandergesetzt und sind entsprechend sensibilisiert, was mit ihren eigenen Daten passiert. Daher werden sie sich auch nicht einfach »abspeisen« lassen Es gilt also Verfahren zu entwickeln, dass bestimmte Daten schnell und umfassend gefunden werden. Im Falle einer Löschung muss das System gesetzliche Aufbewahrungsfristen beachten, auch gilt es sicherzustellen, dass die Daten nicht plötzlich von irgendwoher wiederauftauchen. Das heißt, eventuelle Kopien auf mobilen Endgeräten dürfen nicht wieder ins zentrale System gelangen. Vielmehr darf es gar keine Kopien geben.

Backup und Sicherungskopien

Auch sind Datenkopien, die im Rahmen der Datensicherung entstehen, bei der Löschung zu berücksichtigen. Es gibt unterschiedliche Auffassungen darüber, wie mit bestehenden Backups zu verfahren ist.

Aussagen wie »Falls die Daten im Produktivsystem gelöscht werden, müssten sie zeitnah auch im Backup und weiteren Sicherungsmedien gelöscht werden. Oder auch, dass entsprechende Sicherungskopien zu vernichten seien«, sind rechtlich nicht eindeutig belegt bzw. durch Gerichtsurteile begründet. Die DSGVO ist zwar mit unter schwammig formuliert, es steht aber nirgends, dass alte Backups vernichtet werden müssen.

Fakt ist aber, bei einer Datenwiederherstellung gilt es zu berücksichtigen, dass zu-

vor vernichtete Daten nicht zurück ins Produktivsystem gelangen und nach dem Recovery direkt wieder gelöscht werden. Zudem dürfen Unternehmen Sicherungskopien ausschließlich zum Zwecke von Systemwiederherstellungen verwenden.

Im Übrigen verpflichtet Art. 32.1.c DSGVO Unternehmen dazu Backups zu erstellen: »…die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen…«.

Datenlecks vermeiden und rechtzeitig erkennen

In Artikel 32 fordert die DSGVO zudem eine Pseudonymisierung und Verschlüsselung personenbezogener Daten. Ziel ist es, im Falle einer Sicherheitsverletzung, die Vertraulichkeit und Integrität personenbezogener Daten zu gewährleisten. Der ungewollte Abfluss von personenbezogenen Daten muss zwingend verhindert werden (Data-Loss-Prevention). Das heißt, es gilt umfassende Schutzmechanismen einzubauen. Dies sind unter anderem die Vergabe von Zugriffsrechte nur an relevante Personen sowie der Entzug von nicht mehr benötigten Zugriffsrechten. Eine unkontrollierte Vervielfältigung der Daten sollte ebenfalls nicht möglich sein.

Tritt eine Datenschutzverletzung (Data Breache) auf, ist die wichtigste Anforderung, dass innerhalb von 72 Stunden nach Feststellung, die zuständige Aufsichtsbehörde informiert werden muss sowie die Betroffenen, wenn sie »voraussichtlich« zu einem »hohen Risiko« führt. Anfang Juli war der Hosting-Dienstleister *DomainFactory* zu diesem Schritt gezwungen und musst eine Datenpanne eingestehen.

Letztendlich sind es meist Mitarbeiter, die unachtsam mit den Daten umgehen und diese leichtsinnig weitergeben und in vielen Firmen den größten Schaden anrichten. »Verantwortliche, die keine moderne Lösungen einsetzen und somit das State-of-the-Art-Prinzip nicht erfüllen, müssen dies künftig gut begründen können«, erklärt **Matthias Zacher**, Manager Research & Consulting bei **IDC**. »Denn die DSGVO fordert eindeutig, dass Technologien, die dem Stand der Technik entsprechen bei der Auswahl berücksichtigt werden. Dabei liegt es auf der Hand, dass Unternehmen gegenüber Partnern, Kunden und Aufsichtsbehörden in Erklärungsnot kommen, wenn Mechanismen zur Vermeidung und Erkennung von Datenlecks nicht vorhanden oder veraltet sind und die Datentransparenz nicht gewährleistet ist.«

Die Ausführung »soll dem Stand der Technik entsprechen« ist zwar sehr weich formuliert, die Verordnung soll aber auch noch in zehn Jahren Bestand haben. Alle künftigen Entwicklungen sind hier bereits subsummiert. Laut Zacher bedeutet Stand der Technik, Technik die am Markt verfügbar, sich in der Praxis bewährt hat und auch erschwinglich ist.

Der Anpassung der IT-Systeme kommt eine zentrale Rolle zu, denn ohne Informationstechnologie ist ein effizienter Schutz personenbezogener Daten nicht realisierbar. Zu den State-of-the-Art-Technologien zählt IDC-Manager Zacher: »Next-Gen-Security-Lösungen wie Breach und Leakage-Detection, Intrusion-Detection und Threat-Intelligence sind wertvolle Tools, um Datenlecks möglichst schnell aufzudecken. Diese sind jedoch in der Fläche noch nicht umfassend im Einsatz. Hier sehen wir dringenden Handlungsbedarf.«

Nach IDC Einschätzungen sind Investitionen in den meisten Fällen erforderlich, besonderer Handlungsbedarf besteht im Hinblick auf IT-Security. Grundlegende Anforderungen sind hierbei der sichere Betrieb der IT, ihre permanente Überwachung in Echtzeit und Maßnahmen als Reaktion auf Auffälligkeiten im System. Ein besonderes Augenmerk wird dabei auf Cyber-Security fallen, denn Sicherheitsrisiken und Angriffsszenarien auf personenbezogene Daten lassen sich nur mit moderner Technologie effizient abwehren. Dem Erkennen und Beseitigen von Datenlecks sowie dem Aufspüren und Bekämpfen von Sicherheitsverletzungen kommt dabei eine zentrale Bedeutung zu.

Zu viele Unternehmensdaten sind außerhalb der Firewall

Im Wesentlichen geht es bei der DSGVO um die Regeln, die Unternehmen befolgen müssen, um sicherzustellen, dass persönlich identifizierbare Informationen in gutem Glauben geschützt werden. Mit heutigen Compliance-Tools ist es bisher fast nicht möglich festzustellen, wer wann etwas wusste, vor allem mit Hinblick auf die vielen mobilen Geräte. Verlangt ein Kunde beispielsweise die Löschung seiner Daten, ist die Chance groß, dass diese trotzdem auf einem Tablet, Smartphone oder Außendienst-Notebook noch vorhanden bleiben.

Für viele Unternehmen existieren Daten über die geschäftlichen Aktivitäten hinaus und innerhalb verschiedener IT-Ressourcen. Experten gehen davon aus, dass rund 40 Prozent der Unternehmensdaten heutzutage nicht die zentralen IT-Plattformen erreichen. Das heißt, sie befinden sich nicht hinter der Unternehmens-Firewall.

Um den DSGVO-Anforderungen gerecht zu werden, steht Firmen eine große Aufgabe bevor. ■

Jenseits der Deadline: Datenschutz beeinflusst Datensicherung

Backup und Archiv im Zeichen der EU-DSGVO

Der Hype um den 25. Mai ist erst einmal überstanden. Die meisten Unternehmen dürften sich rechtzeitig gegen Abmahnungen gerüstet haben. Jenseits der Deadline stellen sich nun die konkreten Fragen: Wie kann ich mittelfristig die Auflagen der EU-DSGVO umsetzen? Und wie beeinflusst die EU-DSGVO meine Backups und mein Archiv?

Hannes Heckel, FAST LTA

Die Hauptforderung der EU-DSGVO ist der erweiterte Schutz der Privatsphäre einzelner Personen. Dies umfasst im Wesentlichen drei Punkte, die unterschiedliche Auswirkungen auf Unternehmen haben:

1. Schutz vor Datenverlust und -Missbrauch

Daten mit personenbezogenen Angaben dürfen nicht verloren gehen oder in nicht autorisierte Hände fallen. Wer solche Daten erhebt und speichert, muss dafür sorgen, dass dies nicht passiert – nach »Stand der Technik«.

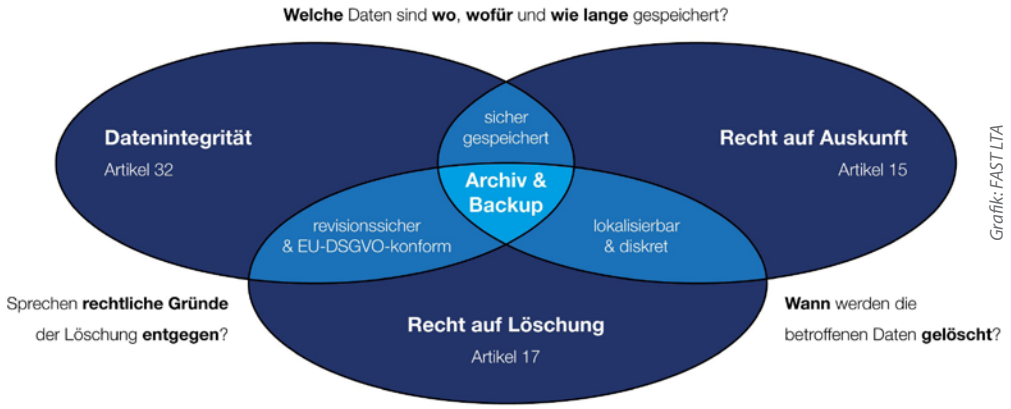
Dies betrifft sowohl Backups als auch Archive. In beiden Bereichen muss vermieden werden, dass (personenbezogene) Daten verloren gehen, etwa durch menschliches Versagen, Manipulation (Ransomware) oder technische Ausfälle.

2. Auskunftsrecht

Wessen personenbezogene Daten gespeichert wurden, hat ein Recht auf Auskunft darüber, zu welchem Zweck, wie lang und wo die Speicherung erfolgt. Dabei gelten die Grundsätze von »Privacy by Default« und »Privacy by Design«. Es dürfen nur die zum eindeutigen Zweck notwendigen personenbezogene Daten gespeichert werden, und nur so lange wie für den Zweck notwendig ist. Systeme und Prozesse müssen so angelegt sein, dass dieses Vorgehen nachvollziehbar ist.

3. Recht auf Löschung

Die vielleicht umstrittenste Regelung ist das »Recht auf Löschung«. Der Begriff suggeriert, dass jeder die vollständige Löschung seiner personenbezogenen Daten verlangen kann – was grundsätzlich auch stimmt. Es gibt jedoch wichtige Einschränkungen. Zum einen muss die Löschung zwar »unverzüglich«, aber eben nicht sofort erfolgen – »unverzüglich« ist dabei im juristischen Sinne wörtlich als »ohne selbstverschuldeten Verzug« zu interpretieren. Zum anderen sind gesetzliche Aufbewahrungsfristen einzuhalten, die im Regelfall stärker sind als das Recht auf Löschung. Die betroffene Person hat dabei ein Recht darauf zu erfahren, zu welchem Zeitpunkt die entsprechenden Daten gelöscht werden (können), was je nach Gesetzeslage durchaus mehrere Jahre in der Zukunft liegen kann.



Die drei Hauptanforderungen der DSGVO betreffen primär die Speichersysteme, die zur Datensicherung eingesetzt werden – also Backup und Archiv.

Die Auswirkungen auf Backup und Archiv

Alle drei Hauptanforderungen betreffen primär die Speichersysteme, die zur Datensicherung eingesetzt werden – also Backup und Archiv. Daten müssen demnach sicher, auffindbar und (nach Einhaltung gesetzlicher Fristen) löschbar gespeichert werden. Im Spannungsfeld zwischen diesen Anforderungen, den Kosten und der Komplexität von IT-Infrastruktur gilt es für IT-Verantwortliche, die richtigen Systeme auszuwählen.

Ein Backup ist kein Archiv: gilt mehr denn je

Weit verbreitet ist immer noch die Praxis, Backup-Instanzen als Archiv zu betrachten. Diese Strategie ist aus mehreren Gründen zu hinterfragen – auch hinsichtlich der EU-DSGVO:

- **Aufblähung des Backups:** Mit den stark ansteigenden Datenmengen werden Zeit und Speicherplatz für Backups immer größer. Je nach verwendeter Software hat das auch Einfluss auf die Kosten durch Lizenzen – mehr Daten, höhere Kosten.
- **Unauffindbarkeit einzelner Datensätze:** Je umfangreicher die Backups werden, desto schwieriger ist es, die Speicherorte einzelner Datensätze exakt zu lokalisieren und diese bei Bedarf zu löschen. Inkrementelle Backups bauen aufeinander auf und sind üblicherweise über mehrere Datenträger verteilt. Full-Backups sind in den seltensten Fällen als Flat-File angelegt, sondern als komplettes Set gespeichert – das sich je nach Größe ebenfalls über mehrere Datenträger erstreckt. Dies steht den Rechten auf Auskunft und Löschen entgegen, ebenso den Privacy-Grundsätzen.
- **Unflexible und unsichere Technologien:** Backups basieren meist auf einer Kombination aus einem NAS und einem Tape-Speicher. Typische (günstige) NAS-Systeme skalieren relativ schlecht. Der zwingende Einsatz von Datenträgern aus identischer Serie erhöht das Risiko für korrelierte Ausfälle. Bit-Rot und Unrecoverable-Read-Errors (URE) können einen Restore unmöglich machen. Zudem sind Rebuild-Zeiten bei heutzutage üblichen Festplattenkapazitäten zunehmend lang und systembelastend. Tape-Speicher skalieren zwar »unendlich«, funktionieren jedoch systembedingt mit langen Zugriffszeiten rein linear. Moderne Recovery-Methoden (bei Veeam z.B. InstantRecovery) sind dabei nicht möglich. Tapes müssen regelmäßig vollständig überprüft bzw. umkopiert werden, um einem schleichenden Datenverlust vorzubeugen, der zwangsweise zu scheiternden Restores führt. Es liegt keine Redundanz vor, es sei denn, es werden mehrere Kopien angefertigt.

Aus diesen Gründen wird schon seit längerem empfohlen, Produktiv- und Archivdaten möglichst früh zu trennen und für die Sicherung Speichersysteme mit integrierter Datensicherung zu verwenden, wie z.B. Gartner im Report *How to Cut Data Protection Costs for Disk-Based File Archives*, 19. September 2016 (nicht öffentlich) ausführt.

Die Neuausrichtung der Speicher-Infrastruktur

Entscheidend sind dabei – entsprechend den obigen Ausführungen – folgende Kriterien:

- Verkürzung des Backups auf ein Minimum, was Aufwand und Kosten spart. Das Backup selbst sollte sowohl schnellen, ständig verfügbaren Online-Speicher als auch kostengünstige, offline-fähige Medien unterstützen.
- Möglichst viele Daten frühzeitig in ein jederzeit skalierbares, File-basiertes Archiv ablegen, was die Auffindbarkeit von Daten und die Möglichkeit, einzelne Datensätze zu löschen, vereinfacht.
- Flexible, moderne Technologien, die über genügend interne Sicherheitsreserven verfügen. Eine Replikation an einen zweiten Standort sollte zur Absicherung gegen Komplettausfall und Verlust leicht möglich sein.

Zusätzlich sollte das Archivsystem über eine Möglichkeit verfügen, als revisionssicherer Speicher Daten mit Aufbewahrungsfristen zu versehen und gegen vorzeitiges Löschen sowie Manipulation wirkungsvoll zu schützen, beispielsweise durch WORM-Versiegelung. Die Zertifizierung sollte möglichst ohne Einschränkungen und Hintertüren gelten und auch das Löschen von Daten enthalten.

Idealerweise stehen alle Anforderungen innerhalb eines einzigen Systems zur Verfügung, das flexible Technologien kombinieren kann, um die unterschiedlichen Vorgaben zu erfüllen. Die Auswahl zwischen schnellen Flash- und kostengünstigen Festplattenspeichern, die Konfiguration als NAS oder VTL, einstellbare Sicherheit jenseits von RAID, und die Möglichkeit der Offline-Lagerung und des Transports einzelner Datenträger, sowie die Ausstattung der langlebigen Infrastruktur mit langfristigen Wartungsverträgen sind dabei zu berücksichtigen. ■

Weitere Informationen

FAST LTA AG
Rüdesheimer Str. 11
80686 München
Tel. 089/89 047-0
E-Mail: info@fast-lta.de
www.fast-lta.de

Hintergründe zu Speichersystemen von FAST LTA und der EU-DSGVO »

RDX-Wechselplattentechnik erfüllt DSGVO-Anforderungen

Datenschutz durch Technikgestaltung

Bild: Tandberg Data

Datenschutz durch Technikgestaltung: Die RDX-Technologie erfüllt die Anforderungen der DSGVO.

Auch wenn die DSGVO nicht die Hauptaufgabe für IT-Verantwortliche ist, sorgt sie insbesondere bei kleinen und mittleren Firmen für Kopfzerbrechen. Datenschutz und Datensicherung sind ohnehin ein Muss, auch vor dem Hintergrund anderer regulatorischer Vorschriften, den Datenschutzempfehlungen des BSI oder etwa Cyberattacken. Um dem besser begegnen zu können, sind beispielsweise Wechselplattensysteme wie RDX geeignet.

von Hugo Bergmann, Overland-Tandberg

Die DSGVO mit ihren 99 Artikeln in elf Kapiteln soll dem Schutz der Privatsphäre und der Verarbeitung personenbezogener Daten dienen. Die gute Nachricht: Viele Bereiche des Datenschutzes werden durch die DSGVO gar nicht neu geregelt, sie erhalten jedoch neue Brisanz durch drohende Strafen bzw. die Furcht vor Abmahnwellen. Immerhin führt die Verordnung dazu, dass auch kleine und mittlere Unternehmen (KMUs) ihre Datenhaltung auf den Prüfstand stellen: Was wird wo gespeichert, gesichert und archiviert? Wie lange werden die Daten vorgehalten?

Laut Art. 25 Absatz 1 der DSGVO sind Unternehmen und Organisationen angehalten, »geeignete technische und organisatorische Maßnahmen« (TOM) in die Wege zu leiten, die darauf ausgelegt sind, die Privatsphäre zu schützen und Datenschutzgrundsätze zu garantieren. Außerdem geht es hier um »Datenschutz durch Technikgestaltung«, und diese obliegt am Ende als Teilaspekt der DSGVO doch der IT-Abteilung.

Datenvorhaltung und Technologiewahl

Im Grundsatz gilt es dabei Wege zu finden, um Daten zu sichern, vorzuhalten und gegebenenfalls zu löschen. Daten müssen zugänglich gemacht werden können, unabhängig davon, ob sie Online-Speicher, Backup oder Archiv sind. Da dies in der Regel über zehn Jahre oder länger gewährleistet werden muss, ist die Wahl einer geeigneten Speichertechnik gut zu überdenken.

Letztlich bleibt jedoch eine Datensicherungsstrategie mit Wechselmedien notwendig, die Auslagerung von Daten auf sicheren, widerstandsfähigen Medien ein Muss. Dazu eignen sich die robusten *RDX*-Medien von **Overland-Tandberg**. Sie kombinieren die Portabilität und Zuverlässigkeit des Bandes mit der Geschwindigkeit einer Festplatte. Auf Dateien kann schnell und direkt im File-System zugegriffen werden, die Systeme sind leicht zu bedienen und kompatibel mit gängiger Backup-Software inklusive Bordmitteln wie *Windows Backup* oder *Apple Time Machine*. RDX-Medien sind dafür äußerst robust gebaut, für eine Lebensdauer von mehr als zehn Jahren konzipiert, vollständig rückwärts- und vorwärtskompatibel und somit immer in einem RDX-Laufwerk ohne technologiebedingten Migrationsaufwand nutzbar, bieten einen Datendurchsatz von bis zu 1,2 TByte/h und Speicherkapazitäten von bis zu fünf TByte pro Wechselmedium und medienübergreifende Sicherungsmöglichkeiten.

Zugangskontrolle und Verschlüsselung

Laut DSGVO müssen die personenbezogenen Daten vor einer »unbefugten Offenlegung« und unbefugtem Zugriff geschützt sein. Dies betrifft letztlich die Möglichkeit, Datenträger einer Policy-basierten Zugangskontrolle zu unterziehen. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Ein weiterer aufgeführter Punkt besteht in der Notwendigkeit der »Pseudonymisie-

rung und Verschlüsselung« personenbezogener Daten und der »Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen«. Dies ist insbesondere für den Datentransport und -austausch ein entscheidendes Kriterium.

Die RDX-Technologie adressiert diese technischen Teilaspekte durch eine Reihe von neueren Entwicklungen. Zunächst basieren RDX-Systeme auf herkömmlicher Festplattentechnik, die den meisten Anwendern insbesondere bei KMU vertrauter sein dürfte als das Magnetband oder Cloud-Lösungen. Die Medien sind uneingeschränkt kompatibel über alle Produktgenerationen hinweg, was bei der Wiederherstellung archivierter Daten ein enormer Vorteil ist.

Mit der *RDX Cartridge Encryptor*-Software (RCE) steht zudem eine freie Software-Anwendung zur Verfügung und erlaubt unkomplizierte Verschlüsselung aller auf RDX gesicherten Daten. Die Software ist für einfache und effiziente Nutzung konzipiert, basiert auf dem AES-256-Encryption-Industriestandard, welcher zugleich *Secure Erase*- nach *NISP*-Standard zur lückenlosen Beseitigung von Daten und Programmen als auch die Funktionalität zum Löschen von Schlüsseln (Cryptographic Key Deletion). Die RDX-Verschlüsselungs-Software bietet damit KMUs eine kostenfreie Lösung für die sichere Speicherung ihrer Daten.

Hardware-Verschlüsselung entspricht höchsten Standards

Mit *RDX PowerEncrypt* steht für die Wechselplattentechnologie auch eine Hardware-basierte Verschlüsselung auf 256-AES-XTS-Standard zur Verfügung. Die Hardware-basierte Verschlüsselungstechnik ist im Vergleich zu Software einfacher zu handhaben, belastet die Prozessorleistung nicht und erzeugt keine Konflikte mit Betriebssystem- und anderen Software-Ständen.

Der schnellste heute verfügbare Super-Computer ist theoretisch in der Lage, pro Sekunde 1014 Schlüssel zu erzeugen und würde damit 3,31 x 1056 Jahre benötigen, um herkömmliche 256-AES-Verschlüsselung zu entschlüsseln. Durch Parallelisierung und zukünftig über Cloud-Services angebotene größere Rechenleistung wird es möglich sein, die herkömmliche 256-AES-Verschlüsselung zu knacken. Mit RDX PowerEncrypt wird die Schlüsseleingabe auf einen Schlüssel pro Sekunde begrenzt, Parallelisierung wird unterbunden und gilt nach heutigem Standard als unknackbar. Die RDX-PowerEncrypt-Verwaltung über den RDX-Manager unterstützt dabei bis zu acht Nutzer mit unterschiedlichen Rechteprofilen und Zugangshierarchien, eine optionale, automatische Laufwerksidentifikation sowie die Analyse der Passwortsicherheit bei der Einrichtung.

Von FIPS bis KPMG – Zertifizierte Lösungen bringen Sicherheit

RDX PowerEncrypt in der ersten Produktversion unterstützt derzeit interne RDX-SATA-III-Laufwerke und -Medien unter Windows. In dieser Konfiguration wird es in 2018 auch FIPS 140-2 validiert werden. Der *FIPS 140-2* (Federal Information Processing Standard) ist ein Standard der US-Regierung und beschreibt die Verschlüsselung und die zugehörigen Sicherheitsanforderungen, die IT-Produkte zur vertraulichen Nutzung erfüllen sollen. Der Standard gewährleistet, dass ein Produkt solide Sicherheitspraktiken wie etwa zugelassene, starke Verschlüsselungsalgorithmen und -verfahren einsetzt. Zudem legt er fest, wie Einzelpersonen oder Prozessabläufe zur Nutzung des Produkts autorisiert werden müssen und wie Module oder Komponenten zur sicheren Interaktion mit anderen Systemen entwickelt werden müssen. Die Validierungsstufe FIPS 140-2 gilt als Zeichen für Sicherheit und Qualität und zertifiziert allen Käufern, dass die Voraussetzungen für Sicherheitsprodukte erfüllt sind.

WORM-Technologie (Write Once Read Many) eignet sich für die Archivierung gemäß regulatorischer Anforderungen. Die *rdxLOCK*-Software wurde jüngst durch die Wirtschaftsprüfungsgesellschaft *KPMG* zertifiziert und damit die integrierte WORM-Funktion für eine Vielzahl an nationalen und internationalen Anforderungsstandards im Buchhaltungs-, Rechnungs- und Steuerwesen frei gegeben.

Diese WORM-Funktion ist damit geeignet, um alle Anforderungen aktueller und zukünftiger Compliance-Regeln wie der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) zu erfüllen.

In der Debatte um die Umsetzung der DSGVO bleiben »geeignete technische und organisatorische Maßnahmen« (Art. 25 Absatz 1) gefordert, die in Hard- und Software und geeigneten Prozessen umgesetzt werden müssen. Die RDX-Technologie mit Wechseldatenträgern, Einzellaufwerken oder Appliances und der entsprechenden Software kann dabei neben anderen Speichertechnologien wertvolle Hilfe leisten: Datenschutz durch Technikgestaltung! ■

Weitere Informationen

Tandberg Data GmbH
Feldstrasse 81
44141 Dortmund
Tel. 00 49 (0)231/54 36-111
www.tandbergdata.com/de/

Datenschutz gilt über den Lebenszyklus der Daten und Technologien

EU-DSGVO – Countdown für die Datensicherheit

Die EU-Datenschutz-Grundverordnung wirkt sich auch auf die Datensicherung aus. Zu erstellen sind Datenschutz- und Datensicherheitskonzepte sowie Folgeabschätzungen. Gegen das Risiko eines Datenverlusts und gegen Verletzungen des Datengeheimnisses gilt es Vorkehrungen zu treffen und zu dokumentieren. »SEP sesam Backup & Recovery« liefert die technische Sicherheit zur Umsetzung der DSGVO.

Andreas Mayer, SEP

Die EU-Datenschutz-Grundverordnung (DSGVO) ist seit dem 25.05.2018 auf Unternehmen und Behörden unmittelbar anwendbar. Das heißt, es können hohe Bußgelder fällig werden. Bis zu zehn bzw. 20 Millionen Euro oder bis zu zwei oder vier Prozent des Jahresumsatzes kann die Strafe betragen. Höchste Zeit für Firmen und Organisationen sich damit intensiver auseinander zu setzen, denn sehr viele waren und sind dafür noch nicht bereit, wie eine Studie der *Nationalen Initiative für Internetsicherheit* (NIFIS) zeigt. 57 Prozent der befragten IT-Sicherheitskräfte erwarteten, dass zum 25. Mai nur 26 bis 50 Prozent der deutschen Unternehmen in der Lage sein werden, die DSGVO-Vorgaben gesetzeskonform umzusetzen. Die DSGVO wirkt sich auf alle Unternehmen aus, die geschäftlich von der EU aus tätig sind bzw. Geschäftsbeziehungen zu Unternehmen/ Organisationen mit Sitz in der EU unterhalten oder Daten in EU-Mitgliedsstaaten sammeln, verarbeiten und speichern. Unternehmen, auch außerhalb der EU, welche Geschäftsbeziehungen zu Unternehmen in der EU und/oder EU-Bürgern mit der Verarbeitung von personenbezogenen Daten unterhalten, unterliegen der DSGVO. Somit sind die Konsequenzen der DSGVO schon fast als weltweit anzusehen. Neu ist auch, dass sogenannte Auftrags-Datenverarbeiter, wie MSP und Cloud-Provider nun auch in der Pflicht sind, die Daten rechtskonform zu behandeln und nicht wie bisher, dass nur der Auftraggeber in der Pflicht war.

Was sind personenbezogene Daten?

Dies sind Daten, welche sowohl berufliche als auch private Informationen über eine Person beinhalten wie Namen, Fotos, E-Mail-Adressen, Bankdaten, Beiträge auf Social-Networking-Websites, medizinische Daten sowie auch die IP-Adressen.

Maßnahmen

Zur DSGVO gehört auch, dass Datenschutz- und Datensicherheitskonzepte sowie Datenschutz-Folgeabschätzungen zu machen sind. Die Datenschutzkonzepte müssen durch technisch-organisatorische Strategien und deren Umsetzung sicherstellen und nachweisen können, dass die DSGVO eingehalten wird. Dies soll auf der Grundlage einer Risikobewertung erfolgen, die auch zu dokumentieren ist ebenso wie auch die hieraus abgeleiteten Maßnahmen in Bezug auf die IT-Sicherheit und die von der IT ausgehenden, unternehmensgefährdenden Risiken durch Datenverlust oder Verletzungen des Datengeheimnisses.

Die Umsetzung muss durch Maßnahmen realisiert werden, die dem aktuellen Stand der Technik entsprechen und dem Datenschutzniveau sowie den Risiken angemessen sind. Dazu sollte eine regelmäßige Soll-/Ist-Analyse mit Risikobewertung und mit einer entsprechenden Datenschutz-/Datensicherheits-Folgeabschätzung kommen, um den Transparenz-, Dokumentations-, ADV- und Sicherheitsmanagementpflichten der DSGVO gerecht zu werden. Datenschutz durch Technik ergänzt die organisatorischen Anforderungen der DSGVO und ist auf den gesamten Lebenszyklus der Daten und Technologien anzuwenden und zu dokumentieren.

Grafik: SEP

Technische Komponente: Backup Software

Die Backup-Software stellt die technische Lösungskomponente dar und muss daher gewisse technische Anforderungen erfüllen sowie technische Mechanismen bereitstellen, um DSGVO-konform zu sein.

Die *SEP sesam Backup & Recovery*-Software liefert die technische Sicherheit, die Sie zur Umsetzung der DSGVO benötigen. SEP sichert herstellerkonform mit einer einzigen Lösung geschäftskritische Informationen in Applikationen, Datenbanken und Systemen sowohl in physikalischen als auch in virtuellen Umgebungen On-Premise und in der Cloud. Aufgrund der immensen Wichtigkeit der business-relevanten Daten wird eine umfassende Business-Continuity-Strategie benötigt, die auf Recovery-Point-Objectives (RPOs) und Recovery-Time-Objectives (RTOs) fokussiert ist, welche essentiell bei einem Disaster-Recovery-Szenario sind.

Die umfassende *SEP sesam Hybrid Backup-* und *Bare Metal Recovery*-Lösung verhindert Datenverlust und kann die gesamte Umgebung nach einem Disaster-Szenario wiederherstellen, beispielsweise bei höherer Gewalt, Hardware-Fehlern, menschlichen Fehlern, Datenkorruption sowie logischen und Software-Fehlern.

Backup-Software mit Verschlüsselung

Die Nutzung des Medienbruchs mittels Offline-Medien (Tape) bei den SEP-Backup-Daten ist bei einer Ransomware-Attacke oft die einzige Möglichkeit, nicht infizierte Daten wiederherstellen zu können, falls die Backup-Daten auf den Disksystemen befallen sein sollten.

Zu den zentralen technischen Elementen gehört die Verschlüsselung. Daher ist zum Beispiel auch bei der technologisch führenden *SEP Si3*-Deduplizierung und -Replikation eine Verschlüsselung möglich. Nach Zerlegen des Datenstroms in Blöcke und der Komprimierung jedes Blocks, lässt sich jeder einzelne Block durch einen beliebig definierbaren Key verschlüsseln. Zur Wiederherstellung der Daten kann der Key in der Datenbank des Backup-Servers hinterlegt werden oder der Dateneigentümer muss eine Rücksicherung mit seinem persönlichen Key autorisieren. Diese Verschlüsselung garantiert *BSI*-Konformität.

Zusätzlich beinhaltet die Lösung eine Vielzahl technologischer Ansätze für die gesetzeskonforme Datensicherheit:

- Verschlüsselung der Backups auf Sicherungsmedien (Band, DataStore, Si3 DedupStore), des Datenstromes (On-Premise und in die Cloud) und der Kommunikation
- Externes Passwort für Rücksicherung nach dem 4-Augen-Prinzip
- Effizientes Disaster-Recovery
- Frei von Spyware/Backdoors (Made in Germany)
- Medienbruch: Unterstützung von Offline- und WORM-Medien
- Herstellerkonforme Datensicherung
- Sicherung der Daten auf verschiedenen Ebenen möglich (z.B. auf Hypervisor- und Applikationsebene)
- Standortübergreifende Datensicherung
- Automatische Migration bzw. Kopie von Sicherungsdaten auf unterschiedliche Sicherungsmedien
- Volle Unterstützung von Open-Source-Betriebssystemen auf Backup-Client- und Backup-Server-Seite
- Gesetzeskonforme Sicherung aller Unternehmensdaten
- Gewährt die Netzwerksicherheit in Firewall-Umgebungen durch Einschränken der Kommunikation und des Datentransports auf wenige, dedizierte Ports
- Geplanter und automatischer Restore auf Stand-by-Systeme zum Verifizieren der Backups (für Audits verwendbar)
- Disaster-Recovery-Tests im laufenden Betrieb inklusive Reporting

Mit SEP sesam sind die Daten 24x7 geschützt und immer verfügbar. Die technologische Lösung kann nur einen Teil der gesamten »Compliance-Lösung« darstellen und muss Hand in Hand an die vorher beschriebenen organisatorischen Maßnahmen, Prozesse, Konzepte, Risiko-Analysen, Dokumentationen, etc. gekoppelt werden, um so zu einer ganzheitlichen »rechtskonformen« Lösung zu werden. Mehr Informationen dazu im White-Paper von Rechtsanwalt und Fachanwalt für IT-Recht Dr. Jens Bücking. ■

Weitere Informationen

SEP AG
Konrad-Zuse-Straße 5,
83607 Holzkirchen
Tel. +49 (0)8024/463 31-0
E-Mail: info@sep.de
www.sep.de/de

Externer Datenschutzbeauftragter: Die größten Irrtümer

Keine Angst vor dem Datenschutzbeauftragten…

Spätestens mit Geltung der DSGVO müssen auch kleinere und mittleren Unternehmen mit einem Datenschutzbeauftragten kalkulieren. Dieser berät zunächst über die Anforderungen und unterstützt bei den zu tätigenden Maßnahmen. Wir erklären hier nochmal, ab wann ein Datenschutzbeauftragter zu benennen ist und räumen mit einigen Irrtümern auf.

Karl Fröhlich

Vor allem in kleineren Unternehmen wird die DSGVO als lästiges Übel gesehen. Datenschutz findet oft nur beiläufig Beachtung und externen Datenschutzbeauftragten wird mit Skepsis begegnet. Geschäftsführer unterliegen zudem immer wieder typischen Irrtümern: »Datenschutz wird leider oft mit IT-Sicherheit verwechselt«, erklärt **Isabelle Fircks**, Geschäftsführerin des Datenschutzdienstleisters **PROLIANCE** (Datenschutzexperte.de). »IT-Sicherheit deckt letztlich nur einen Teil des eigentlichen Datenschutzes ab. Für jede Unternehmensabteilung – etwa Buchhaltung, Personal oder Vertrieb – bestehen besondere datenschutzrechtliche Vorgaben, die für IT-Abteilung meist nicht überschaubar sind.«

Kleine Unternehmen gehen regelmäßig davon aus, dass sie keinen Datenschutzbeauftragten benötigten. »Doch bereits ab zehn Mitarbeitern, die Zugriff auf personenbezogene Daten haben, beispielsweise über Outlook, ist ein Datenschutzbeauftragter vorgeschrieben«, stellt Fircks klar. »Als Mitarbeiter zählen auch Teilzeitkräfte, Freelancer und Praktikanten.«

»Wir wurden noch nie kontrolliert« ist auch eine beliebte Ausrede. Meist rechnet man nicht damit, dass eine Kontrolle das eigene Unternehmen trifft, bis es passiert. »Schon vor dem 25. Mai 2018 waren die Aufsichtsbehörden restriktiv«, sagt Fircks. »Nach Geltung der DSGVO muss mit einem noch härteren Durchgreifen gerechnet werden.«

Datenschutzbeauftragter: Nicht jeder ist zulässig

Die DSGVO regelt die Benennung, Stellung und Aufgaben des Datenschutzbeauftragten im Artikel 37, 38 und 39. Vereinfacht ausgedrückt, kann jeder Datenschutzbeauftragter (DSB) werden, der sich, über Schulungen, die dafür nötige fachliche Qualifikation aneignet. Dabei kann es sich um einen internen Mitarbeiter handeln oder einen externen Dienstleister.

Der DSB berichtet unmittelbar an die Geschäftsleitung oder Vorstandsebene. Ihm kommt eine Kontrollpflicht zu, daher ist sicherzustellen, dass ihm keine Weisungen erteilt werden und der DSB völlig unabhängig arbeiten kann. Zudem darf der DSB wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Ein interner DSB erwirbt mit der Ernennung quasi den Stellenwert eines Betriebsrates.

Foto: Proliance

Isabelle Fircks
Proliance

»Datenschutz wird leider oft mit IT-Sicherheit verwechselt.«

Ausbildung zum DSB

Die Ausbildung zum Datenschutzbeauftragten dauert unterschiedlich lange: Online-Akademien sprechen davon, dass der Kurs in 48 Stunden abzuschließen sei. Weiterbildungsinstitute, die *IHK* und der *TÜV* bieten Seminare von drei bis fünf Tagen an.

Die Gebühren belaufen sich auf ungefähr 1.700 bis 2.100 Euro (netto). Die Online-Anbieter *datenschutz.net* und *datenschutz.com* verlangen für zwei Personen 1.750 Euro netto. Unser Chefredakteur hat hier sein Zertifikat in einem Selbstversuch erworben.

Sein Resümee: »Im Grunde ist es egal, auf welchen Weg Ihr das Zertifikat erwerbt. Die Kurse vermitteln nur die Basics. In Vor-Ort-Seminaren trifft man Gleichgesinnte, mit denen man dann Netzwerken könnte. Für einen Neuling ist der Fragenkatalog endlos.«

Der DSB kann andere Aufgaben und Pflichten wahrnehmen, allerdings muss gewährleistet sein, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Das heißt, Mitglieder der Geschäftsleitungen können nicht zum DSB benannt werden. Sie würden sich selbst kontrollieren und dies ist ausgeschlossen.

Da der DSB einen tiefen Einblick ins Unternehmen erhält, ist er zur Wahrung der Geheimhaltung und Vertraulichkeit verpflichtet. Speziell die Beauftragung eines externen DSB hat natürlich etwas mit Vertrauen zu tun. Derzeit muss man aber fast nehmen, was man kriegen kann. Die DSGVO hat alle Datenschutzfirmen an den Rand ihrer Kapazitäten gebracht – und vielfach darüber hinaus.

Vorsicht: IT-Dienstleister als Datenschutzbeauftragter

Nicht nur aus Ermangelung an Alternativen, könnte es durchaus praktisch sein, wenn der IT-Dienstleister die Aufgaben des Datenschutzbeauftragten mit übernehmen könnte. Er kennt das Unternehmen und die IT-Struktur, was durchaus als Vorteil gesehen werden kann. Natürlich benötigt er einen Mitarbeiter mit der entsprechenden Qualifikation und Erfahrung. Zulässig ist es trotzdem nicht.

Stephan Hansen-Oest, Rechtsanwalt mit Spezialisierung auf Datenschutz und IT-Recht, erklärt in seinem Datenschutz-Guru-Podcast, dass hier mit einem Interessenskonflikt zu rechnen sei. Laut Artikel 39.1b DSGVO überwacht der DSB die Einhaltung der Verordnung. Betreut ein IT-Dienstleister eine Firma umfassend, hat er auch mit Datenverarbeitung zu tun und würde sich demnach selbst kontrollieren.

Auch die Möglichkeit, den Datenschutzbereich in eine Tochterfirma auszulagern, sehen Anwälte und Aufsichtsbehörden kritisch. Eine Unabhängigkeit gegenüber der Muttergesellschaft, die vermutlich das Geld hat, könne nicht glaubhaft gewährleistet werden. Da es sich um ein EU-Gesetz handelt, seien die Aufsichtsbehörden auch um eine einheitliche Regelung bemüht. Daher ist davon auszugehen, dass alle im Zweifel eher auf Nummer sicher gehen.

Datenschutzbeauftragter: Kosten und Nutzen

Die Kosten für einen DSB variieren je nach Unternehmensgröße, Branche und Geschäftsfeld. In der Regel ist mit einer monatlichen Pauschale zu rechnen sowie mit einem einmaligen Honorar für das Anfangs-Audit und die dazugehörige Dokumentation (Verfahrensverzeichnis, TOM). Der Einstieg für kleinere Betriebe wie Handwerker, Werkstätten und Einzelhändler beginnt bei Audit-Gebühren von zirka 1.250 Euro und monatlich 150 Euro. Ärzte, Apotheker, Online-Shops und kleinere IT-Firmen sollten mit über 2.000 Euro und 350 Euro monatlichen kalkulieren. Unternehmen mit mehr als 100 Mitarbeitern sind ab 3.000 Euro und ab 500 Euro/mtl. dabei. Wobei diese Preise eher als Anhaltspunkt gesehen werden sollten.

Die Marktlage spielt den Dienstleistern in die Karten. Gleichfalls darf auch der Aufwand, der hinter einer Bestandsanalyse steht, nicht unterschätzt werden. Auch steht der DSB mit seinem Namen für die Richtigkeit der Angaben. Datenschutz ist kein Freundschaftsdienst. Zudem muss sich der DSB immer auf dem Laufenden halten, auch über die Entwicklungen in den Branchen seiner Kunden. Es ist nicht damit getan, einmal ein Zertifikat zu erwerben. Vor allem für KMUs ist ein externer Dienstleister eigentlich eine sinnvolle »Anschaffung«.

Und auch für Firmen, die keinen DSB benennen müssen, ist es ratsam für die Bestandsaufnahme einen Experten zu Rate zu ziehen. Den einmaligen Ausgaben sollte eine Zeitersparnis gegenüberstehen und man hat dann eine korrekte Basis. Auf dieser können Betriebe aufbauen bzw. hat Bestand bis zur nächsten großen Überarbeitung der Datenschutzverordnung. ■

Datenschutz-Wissen aufbauen

Die Prüfung zum Datenschutzbeauftragten sollte eigentlich jeder bestehen, der den Lehrgängen ein bisschen Aufmerksamkeit geschenkt hat. Die Probleme kommen erst in der Praxis. Checklisten und Muster gehören meist zu den Seminarunterlagen. Mit der praktischen Anwendung steht der Datenschutznovize aber erstmal alleine da. Die Anforderungen sind hoch, die Vorgaben aber eher unkonkret. Daher ergeben sich viele Fragen und Unsicherheiten. Einer der hier hilft, ist **Stephan Hansen-Oest**, Rechtsanwalt mit Spezialisierung auf Datenschutz und IT-Recht, der im Web unter datenschutz-guru.de sein Wissen weitergibt. Ein großer Teil ist frei zugänglich, seinen Coaching-Mitgliedern bietet er aber eine noch viel umfangreichere Download-Bibliothek. Monatlich findet ein Live-Webinar zu einem aktuellen Thema statt. Ein Novum sind die sogenannten Office-Hours. Das darf man sich als eine Art Telefonsprechstunde vorstellen. Fragen können vorab eingereicht oder live »on Air« gestellt werden. Natürlich sind Aufzeichnungen verfügbar und auf Wunsch erhält der Teilnehmer auch eine Fortbildungsbescheinigung. Kosten: ca. 41 Euro für 1 Monat, 429 Euro für 12 Monate (netto).

Anzeige

DATENSCHUTZEXPERTE.DE
einfach. sicher. schnell.

Datenschutzexperte.de ist ein junges Unternehmen aus dem Legal Tech Bereich aus München und eine auf den betrieblichen Datenschutz spezialisierte Unternehmensberatung. Als externer Datenschutzbeauftragter beraten wir unsere Kunden – kleine und mittlere Unternehmen aller Branchen – dabei, die Anforderungen der europäischen Datenschutzgrundverordnung (EU-DSGVO) mit digitalen Datenschutzkonzepten einfach und sicher umzusetzen. Dabei revolutionieren wir den Datenschutz auf eine digitale Art und Weise.

Mit unserem erfahrenen Management-Team und mehr als 30 engagierten Mitarbeitern, bestehend aus einer Vielzahl von TÜV/DEKRA zertifizierten Datenschutzbeauftragten, sind wir bereits heute eines der größten Legal Tech Unternehmen in Deutschland und Europa. Unsere Mitarbeiter unterstützen Hunderte von Unternehmenskunden in Europa mit individuellen und vor allem praxistauglichen Konzepten dabei, die Maßnahmen pragmatisch und einfach in den Geschäftsbetrieb zu integrieren.

Unsere eigens entwickelte SaaS-Kundenplattform »myDSE« ermöglicht es unseren Kunden den Unternehmensdatenschutz vollständig digital und somit einfach, sicher und schnell zu verwalten. Darüber hinaus nimmt sie unseren Mitarbeitern repetitive Aufgaben ab, damit sie den Fokus vollständig auf eine ganzheitliche Datenschutzberatung zu attraktiven Preisen legen können.

Zu unseren Kunden gehören Unternehmen aus einer Vielzahl unterschiedlicher Branchen und Reifegrade – vom innovativen Startup bis zum etablierten Traditionsunternehmen. Darüber hinaus kooperieren wir mit einer Vielzahl von Branchenverbänden und Organisationen, die unsere Dienstleistungen an Ihre Partner weiterempfehlen. Treten Sie gerne direkt mit uns in Kontakt.

Isabelle Fircks
Geschäftsführerin

Bei Fragen stehen wir Ihnen jederzeit telefonisch unter **+49 89/250 039 220**, per E-Mail **hatz@datenschutzexperte.de** oder direkt über unser Kontaktformular unter **www.datenschutzexperte.de** zur Verfügung!

Anzeige

43 – Sabine Noack: Datenschutz und IT-Beratung

Die DSGVO ist bereits seit Ende Mai in Kraft getreten, dennoch sind sich auch heute noch viele Kleinunternehmer unsicher, in wie weit sie überhaupt von der DSGVO betroffen sind, ob sie einen Datenschutzbeauftragten benötigen und in wie weit sie bereits DSGVO konform arbeiten. Entgegen der Annahme vieler insbesondere kleiner Unternehmen hat man mit einer Standard-Datenschutzerklärung auf der Firmen-Webseite noch lange nicht alle Anforderungen der DSGVO umgesetzt und dann drohen neben wettbewerbsrechtlichen Abmahnungen unter Umständen auch hohe Strafen durch die für den Datenschutz zuständigen Aufsichtsbehörden.

Ich biete Ihnen eine umfassende Erstanalyse und Bewertung aller Datenschutz-relevanten Prozesse Ihres Unternehmens mit abschließendem Statusbericht und einer ToDo-Liste aller offenen Aufgaben an. Danach können Sie entscheiden, ob Sie mich für eine feste Monatspauschale zu Ihrer externen Datenschutzbeauftragten bestellen wollen und wieviel Unterstützung Sie unabhängig davon in Form von Datenschutzberatungs-Paketen benötigen.

Dazu gehören u.a. das Etablieren eines an Ihr Unternehmen angepasstes Datenschutz-Konzept und ggf. eines Datenschutz-Teams. Ich unterstütze beim Erstellen und Aktualisieren der notwendigen Dokumentation, Verarbeitungsverzeichnis, TOMs, Datenschutz-Handbuch, AVV sowie Ihren Informations- und Auskunftspflichten, u.a. durch anpassbare Musterdokumente. Ich schule Ihre Mitarbeiter und beantworte Fragen zu Datenschutz und Datensicherheit. Dadurch entlasten Sie Ihre Mitarbeiter und können sich wieder mehrheitlich Ihrem Kerngeschäft widmen.

Als Ihr externer Datenschutzbeauftragter fungiere ich darüber hinaus als Ansprechpartner Ihres Unternehmens für die Aufsichtsbehörden und erstelle den geforderten jährlichen Datenschutz-Statusbericht. Vereinbaren Sie einen Termin für ein kostenloses Erstgespräch und machen Sie Ihr Unternehmen DSGVO konform.

Dipl. Inform.
Sabine Noack
DSC zertifizierte externe Datenschutzbeauftragte für Ihr Unternehmen

Web: **www.4ty3.de**,
E-Mail: **info@4ty3.de**
Tel. **+49 89/202 397 52**,
Mobil. **+49 151/425 311 76**

Anzeige

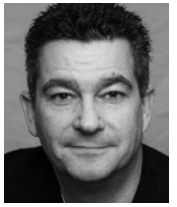
Datenschutz für Kleinbetriebe und kleine Unternehmen

Sie sind sich nicht sicher, was die DSGVO für Ihren Betrieb genau bedeutet? Was damit auf Ihr Unternehmen zukommt und welche Maßnahmen letztendlich umzusetzen sind? Dann sind Sie hier richtig: Mit meinen Datenschutz-Service habe ich mich vor allem auf kleine Firmen spezialisiert.

Auch wenn Sie von Ihrer Unternehmensgröße her keinen Datenschutzbeauftragten benennen müssen, benötigen Sie eventuell Rat und Unterstützung, sei es bei der Dokumentation, dem Verfahrensverzeichnis sowie den technischen und organisatorischen Maßnahmen. Als Redakteur liegt mir das Dokumentieren im Blut.

Bedenken Sie, die DSGVO betrifft nicht nur Ihren Internetauftritt oder den Umgang mit Kundendaten, sondern auch die personenbezogenen Daten Ihrer Mitarbeiter, Lieferanten und Partner.

Sollte es nötig sein, agiere ich für kleine Firmen auch als externer Datenschutzbeauftragter zum leistungsgerechten Pauschalpreis und persönlicher Betreuung.



Karl Fröhlich
DSC zertifizierter externer Datenschutzbeauftragter

Setzen sie sich gerne mit mir in Verbindung, telefonisch unter **+49 89/740 03 99** oder per Mail an **karl[at]KarlFroehlich.de**.

Jan Mentel, Analyst, Crisp Research im Interview zur DSGVO

DSGVO: »Die vielen Schwachstellen sind eine Gefahr«

Die EU-Datenschutz-Grundverordnung ist gut gemeint, bringt aber auch zu viele Ungereimtheiten mit sich. Kleine Firmen fühlen sich allein gelassen und stehen zum Teil vor unlösbaren Aufgaben. Die großen Techunternehmen gehen dagegen gelassen an die DSGVO heran. Jan Mentel bezeichnet dies als geradezu grotesk. Wir sprachen mit dem Analysten des Beratungsunternehmens Crisp Research, über die Nachteile der DSGVO.

Karl Fröhlich

In Ihrem Zwischenfazit zur EU-DSGVO üben Sie einige Kritik. Während sich die großen Unternehmen über fast alles hinwegsetzen, leiden die Kleinen unter der Umsetzung.

Mentel: Das ist schon grotesk. Auf der einen Seite wurde genau aus diesem Kontext die DSGVO ins Leben gerufen, um den Nutzern mehr Schutz, Transparenz und Rechte einzuräumen. Ohne Schlupflöcher, am Verbraucher orientiert, um nicht den Lobbyisten in die Karten zu spielen. Doch im Endeffekt schlägt es in die andere Richtung um, da die DSGVO nicht präzise ausformuliert wurde.

Jan Mentel, Crisp:

»Nur die Global-Player profitieren von der DSGVO.«

Daher gehen die großen Technologieunternehmen gelassen an die DSGVO heran. Die zentralen Herausforderungen hat das europäische Parlament nicht definiert, geschweige denn berücksichtigt und aufbereitet.

Somit ist es wieder möglich, dass zum Beispiel *WhatsApp* Daten an den Mutterkonzern weiterleiten kann und *Facebook* eifrig an Gesichtserkennungs-Tools tüftelt. Jedoch werden Marketing- und Werbeaktivitäten kleiner und mittelständischer Unternehmen blockiert.

Was muss aus Ihrer Sicht passieren?

Mentel: Fakt ist, es bedarf klarer, fairer und spezifischer Regeln für alle, bezüglich der Verwendung von Daten, auch vor dem Hintergrund technischer Neuerungen. Neben der mangelhaft ausformulierten Verordnung, die viel Spielraum für die großen Anbieter lässt, wurde es bei zentralen Fragen vor allem vernachlässigt, um die Ecke zu denken. Was ist, wenn Verbraucher das »Recht auf Vergessen werden« nicht in Kauf nehmen?

Dadurch, dass Daten nicht gelöscht werden können, wenn Verbraucher dies nicht veranlassen, entwickelt sich ein riesiger Datenpool. Unternehmen müssen alle Aufzeichnungen aufbewahren, so dass ein Verbraucher drei Jahre nach der Einwilligung seine Einwilligung widerrufen kann, dass kein Datenhandel nachgewiesen, und dass der Datensatz gelöscht werden kann. Ein gefundenes Fressen für Hacker. Angriffe auf diese Datenpools werden um ein Vielfaches steigen.

Das heißt, die DSGVO ist noch zu unausgegoren und birgt zu viele Nachteile?

Mentel: Die Autorität und Aufgabenteilung des europäischen Datenschutzamtes ist noch nicht genau ausgearbeitet. Die Anforderungen an die Datenspeicherung, die Einwilligung zur Nachverfolgung und die Beweisführung gemäß der DSGVO sind so umfassend, dass, wenn überhaupt, nur wenige Unternehmen in der Lage sind, sich selbst als konform zu betrachten.

Und das bedeutet, dass Unternehmen in einer zunehmend vernetzten Welt wirklich in Gefahr sind, wenn das Datenschutzamt darüber willkürlich entscheidet, was falsch oder richtig ist. Dies bedeutet wiederum, dass die Zahl der illegalen Datensammler und -verkäufer in die Höhe schießen wird und das ist für die Verbraucher ein absoluter Nachteil.

Lesen Sie das ganze Interview mit Crisp-Research-Analyst Jan Mentel, hier auf speicherguide.de. ■

Newsletter-Abonnenten erhalten die neue Ausgabe jeweils »linkfrisch« an ihren Mail-Account. Registrieren Sie sich bitte hier.
Beachten Sie auch unser Archiv im Download-Bereich.

storage-magazin.de
eine Publikation von speicherguide.de GbR
Karl Fröhlich, Ulrike Rieß
Ginsterweg 12, 81377 München
Tel. +49 (0) 89-740 03 99
E-Mail: redaktion@speicherguide.de

Chefredaktion, Konzept:
Karl Fröhlich (verantwortlich für den redaktionellen Inhalt)
Tel. 089-740 03 99
E-Mail: redaktion@speicherguide.de

Redaktion:
Karl Fröhlich

Schlussredaktion:
Brigitte Scholz

Layout/Grafik:
Uwe Klenner, Layout und Gestaltung,
Rittsteiger Str. 104, 94036 Passau,
Tel. 08 51-9 86 24 15
www.layout-und-gestaltung.de

Titelbild:
iStockphoto.com / PeopleImages

Mediaberatung:
Claudia Hesse,
Tel. +41 (0) 41 - 780 04 86
E-Mail: media@speicherguide.de

Webkonzeption und Technik:
Günther Schmidlehner
E-Mail: webmaster@speicherguide.de

Unser Team

Karl Fröhlich,
Chefredakteur
speicherguide.de

Claudia Hesse,
Mediaberatung
speicherguide.de

speicherguide.de
Das Storage-Magazin

Wir empfehlen zur vollständigen Funktionalität des eBooks »Acrobat Reader«, ab Version 9