Eine Publikation des Reflex Verlages zum Thema

5 vor EU-DSGVO

Datensicherheit

IT-Sicherheit ist die „Conditio sine qua non", um diese Bedingung dreht sich alles. Sind Dateien beispielsweise auf dem Laptop verschlüsselt, muss das auf mobilen Endgeräten ebenso der Fall sein. Always-on-Dateiverschlüsselungen übernehmen die Daten.

Seite 6

Finanz- und Forderungsmanagement

Nach EU-DSGVO wird der Umfang der erhobenen Daten auf ein Minimum reduziert. Besonders im Finanz-, Versicherungs- und Forderungsbereich sollen bis auf die wirklich relevanten Datensätze keine weiteren Informationen gesammelt, verarbeitet und gespeichert werden.

Seite 8

Recht

Gebot für alle internen Maßnahmen sind die möglichen rechtlichen Konsequenzen bei Verstößen gegen die EU-DSGVO. Im Einzelnen betrifft dies insbesondere alle Datenverarbeitungsprozesse, die personenbezogene Daten betreffen.

Seite 13

FEBRUAR 2018

REFLEX Verlag

Balance aus Risiken und Chancen

Datenschutz kann als Drahtseilakt und Gratwanderung zwischen den Anforderungen in Zeiten der Digitalisierung, dem Wunsch nach Datenkontrolle und dem Erfüllungsgrad zunehmender Bürokratien verstanden werden. Die Frage nach der Balance erscheint berechtigt. Ob es den Schöpfern der EU-DSGVO gelungen ist, ein Werkzeug zu kreieren, das faire Risiken und Chancen abwägt, bleibt zu hoffen. Für den Schutz der persönlichen Daten ist es allemal ein Durchbruch. Jedenfalls besteht bis zum Startschuss am 25. Mai 2018 noch Gelegenheit, sich mit der Sicherheit und dem Schutz eigener und fremder Daten kritisch auseinanderzusetzen. Das Gesetz wird sowohl Licht in die „Shadow-IT“ bringen, als auch durch klare Regulierungsvorschriften mehr Kontrolle zulassen und Vertrauen schaffen. An der zunehmenden dynamischen Entwicklung der Digitalisierung wird die EU-DSGVO nichts ändern.

Karl-Heinz Möller
Chefredakteur

DATENSICHERHEIT

3 Leitartikel
Am 25. Mai diesen Jahres tritt die EU-DSGVO in Kraft. Die neue Datenschutzverordnung ist diesmal kein Papiertiger, sondern ein Monster mit scharfen Zähnen. Beste Vorbereitung in Unternehmen ist zu empfehlen, denn die Strafen bei Vergehen sind drastisch.

6 IT-Sicherheit Datentransfer
Für alle personenbezogenen Daten gelten neue Bestimmungen. Ob Verwendung, Speicherung oder Weitergabe – für jede Aktivität ist Einverständnis des Betroffenen einzuholen. Die Vorgänge müssen sauber dokumentiert, betreut und sicher verwahrt werden.

7 IT-Sicherheit Prävention
Stündlich werden Milliarden von Files durch die Netze geschickt, und das Augenmerk gilt insbesondere persönlichen Daten. Seien es Telefonnummern, Adressen, Codes oder digitale Schlüssel, als sensible Informationen müssen sie mit höchster Sicherheitspriorität behandelt werden.

LÖSUNGEN

8 Finanz- und Forderungs-Systeme
Daten aus Finanz-, Versicherungs- und Forderungsgeschäften gehören zu den Informationen mit großer Sicherheitsrelevanz. Vor, in und nach Transaktionen werden vor allem für personennahe Daten ausführliche Vorgehensweisen gesetzlich vorgezeichnet.

10 ePrivacy
Regeln für Datenschutz machen besonders dann Sinn, wenn die persönlichen Daten im Rahmen der elektronischen Kommunikation sicher verarbeitet werden. In neuen Datenschutzkonzepten sind diese Anforderungen bereits eingeflochten.

11 IT-Managementsysteme
Die umfangreichen Vorgaben der EU-DSGVO in ein IT-Management zu integrieren beziehungsweise ein solches zu implementieren erscheint als eine sinnvolle Investition. Auf diese Weise sind regelbasierte gesetzeskonforme Abläufe garantiert.

BEST PRACTICE

12 Compliance und Weiterbildung
In der Komplexität und im Umfang des neuen Gesetzes spielen Aspekte der Complience eine bedeutende Rolle. Um sie zu umzusetzen, bedarf es des ausführlichen Trainings und der Weiterbildung.

13 Rechtsaspekte
Gesetze wie die EU-DSGVO zu verstehen und richtig gesetzeskonform umzusetzen, ist die vornehmliche Aufgabe von Juristen. Vor allem sind nur sie in der Lage, Stolpersteine und Fallen zu erkennen.

Das Papier der Publikation, die im aufgeführten Trägermedium erschienen ist, stammt aus verantwortungsvollen Quellen.

LEITARTIKEL

Countdown für den großen Daten-Check

Das neue EU-Datenschutzrecht klopft immer lauter an die Tür. Bis zum 25. Mai dieses Jahres können Unternehmen und Behörden noch ihre IT-Systeme und Organisationen anpassen. Dann läuft eine zweijährige Übergangsfrist ab, und die nationalen Aufsichtsbehörden werden beginnen, die EU-Datenschutz-Grundverordnung (EU-DSGVO) durchzusetzen. Alte nationale Datenschutzregeln laufen dann aus oder werden angepasst. Deutschland hat bereits ein neues nationales Datenschutzanpassungsgesetz verabschiedet, weitere europäische Staaten folgen.

Von Karl-Heinz Möller

Mit dem tiefen Eintauchen in das Informationszeitalter und der sich dynamisch entwickelnden technischen Möglichkeiten – die Rede ist von Speicherung großer Informationsmengen, automatischer Übermittlung und intelligenter Auswertung der Informationen – avancieren die in diesem Prozess emsig gehandelten personenbezogenen Daten zum „Öl der Zukunft“. Neue Geschäftsmodelle entstehen per Analyse und Transformation der Datensätze. Die daraus resultierenden Strategien führen zu Wettbewerbsvorteilen und stärken die Positionen der agierenden Unternehmen.

Im Umfeld der nationalen Vorschriften – hierzulande greift bisher das nationale Bundesdatenschutzgesetz BDSG – werden künftig die Regeln der EU-DSGVO verbindlich gelten. Sie harmonisieren innerhalb der Europäischen Union den Datenschutz. Mit den neuen rechtlichen Rahmenbedingungen zum Schutze und zur Sicherheit der Daten geht eine erhebliche Verschärfung der Bedingungen einher. Einschließlich empfindlich hoher Strafzahlungen für Unternehmen in Millionenhöhe, soweit sie die die Regeln missachten.

> *Data-Governance ist vorbild für ein gesetzeskonformes Datenschutzkonzept.*

Unternehmen werden ihre Geschäftsprozesse anpassen müssen

Für jedes Unternehmen, das sensible Daten verarbeitet – und das sind praktisch alle – ergeben sich damit eine Reihe neuer Aufgaben. Unternehmen müssen ihre Geschäftsprozesse verändern, Daten löschen oder konsolidieren, Einwilligungstexte überarbeiten, neue Software implementieren und alles penibel dokumentieren. Großunternehmen verfügen in der Regel über eigene Datenschutzabteilungen und große Budgets, um professionelle und großangelegte Datenschutz-Management-Systeme aufzubauen beziehungsweise neue Module in ihre vorhandenen IT-Lösungen einzufügen. Mittelständlern fehlen hingegen oft diese Ressourcen.

Darüber hinaus führen Unsicherheiten hinsichtlich der Handhabung der Regeln durch die Aufsichtsbehörden dazu, dass – oft in einem Vakuum zwischen Zaudern und Aktionismus – mittelständischen Unternehmen innovative Projekte vorerst zurückstellen.

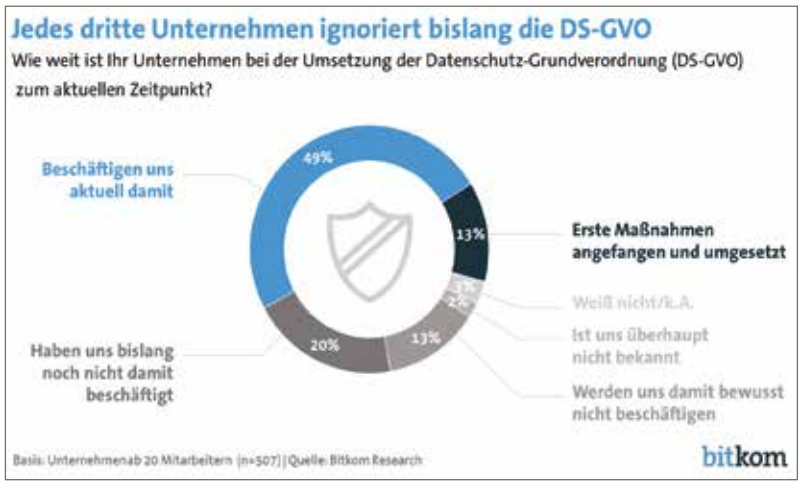
Um den Anforderungen der Datenschutzgrundverordnung ge- ▶▶▶

GASTBEITRAG

Hohes Gut: einheitliche Datenschutzregeln

Mit der Datenschutzgrundverordnung haben wir erstmals ein in den zentralen Punkten einheitliches Datenschutzrecht in der Europäischen Union. Es gilt auch für Unternehmen aus Drittstaaten. Das allein ist sehr positiv, sagt Achim Berg, Präsident des Digitalverbands Bitkom

Mit der Verordnung ist für Unternehmen aber auch ein erheblicher organisatorischer Aufwand verbunden. Sie müssen zahlreiche neue Informations- und Dokumentationspflichten umsetzen. Völlig neu sind gesetzliche Vorgaben wie die Berücksichtigung des Datenschutzes bei der Produktentwicklung (Privacy by Design) oder die Durchführung einer Datenschutz-Folgenabschätzung. Solche Maßnahmen in einem Unternehmen zu integrieren, ist keine leichte Übung. In Kleinunternehmen fehlen dafür häufig das fachliche Know-how und das Bewusstsein für die Notwendigkeit. In großen Unternehmen ist der Aufwand sehr hoch. Viele Unternehmen haben daher Schwierigkeiten, die Datenverarbeitung bis zum Stichtag 25. Mai 2018 gesetzeskonform anzupassen.



Unternehmensbefragung im Auftrag des Digitalverbands Bitkom, September 2017.

Viele Unternehmen sind hinterher

Im September 2017 hatte sich ein Drittel der Unternehmen in Deutschland noch gar nicht mit der Datenschutzgrundverordnung beschäftigt. Nur 13 Prozent hatten damals mit ersten Umsetzungsmaßnahmen angefangen. Viele wünschen sich deshalb zusätzliche Auslegungshilfen durch die EU, durch die Datenschutzbehörden oder Praxisleitfäden von Verbänden. Für nicht wenige rächt sich jetzt, dass sie das Thema Datenschutz zu lange vernachlässigt haben. Oft sind bis heute nicht einmal einfachste organisatorische Voraussetzungen geschaffen worden. Die Folge: Vielen Unternehmen in Deutschland drohen Millionen-Bußgelder.

Aber auch für Unternehmen, die Maßnahmen ergriffen haben, bleibt Rechtsunsicherheit. Sie können nicht einschätzen, wie streng die jeweilige Datenschutzbehörde die neuen Regelungen auslegt und wie genau sie die Umsetzung der neuen Vorgaben in Unternehmen prüfen wird. Viele hoffen, dass sie weiterhin unter dem Radar der Behörden fliegen können. Sich zu verstecken ist aber keine Lösung. Die Unternehmen müssen etwas tun.

Fairer Wettbewerb durch die Datenschutzgrundverordnung

Langfristig bietet die Datenschutzgrundverordnung mehr Rechtssicherheit für Unternehmen. Das Ziel der Verordnung ist es, einen modernen und einheitlichen Rechtsrahmen in Europa zu schaffen. Das vereinfacht die Arbeit von Unternehmen, die in mehreren europäischen Ländern tätig sind, und sorgt auch für fairen Wettbewerb zwischen den Standorten. Vorteile der Verordnung sind vor allem die einheitlichen Wettbewerbsbedingungen in der EU. Davon können gerade auch kleine und mittlere Unternehmen profitieren.

recht zu werden, und um den Aufwand kalkulierbar zu machen, kann die Investition in eine spezielle Software lohnen. Sie beinhaltet bereits den neuesten Umsetzungsstand des Gesetzes und alle wesentlichen Informationen – zum Beispiel Muster zur Beantwortung einer aufsichtsbehördlichen Anfrage.

Sensibler Umgang mit personenbezogenen Daten

Wie der Umgang mit Informationen im Unternehmen zu erfolgen hat, gibt in Grundzügen der Aufbau der EU-DSGVO vor. Das „Gesamtwerk" ist ein komplexes Gesetzbuch mit elf Kapiteln und 99 Paragraphen („Artikeln"). Wegen ihrer besonderen Relevanz in der unternehmerischen Praxis finden die Artikel 5 und 32 die größte Beachtung. Artikel 5 beschreibt die Grundsätze bezüglich der Verarbeitung personenbezogener Daten. Im Artikel 32 steht die Sicherheit der Verarbeitung im Mittelpunkt.

Kernpunkte wie diese sind die DNA der EU-DSGVO. Sie sind der Schlüssel für ein gesetzeskonformes Datenschutzkonzept. Bestens geeignet für den Entwurf eines solchen Modells ist eine existierende Data Governance. Formuliert finden sich dort rechtliche Vorgaben wie Zuständigkeiten für Daten, Unterteilung der Daten, Definition von Lebenszyklen.

Checklisten systematisieren die Schritte zur Umsetzung der EU-DSGVO

Da der Fokus auf den personenbezogenen Daten liegt, ist eine Analyse aller Daten notwendig, die dafür in Frage kommen. Eine Checkliste beginnt mit der Klärung, was überhaupt unter personenbezogenen Daten zu verstehen ist. Laut EU-DSGVO sind „personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Der Begriff „identifizierbar" wird unter verschiedenen Aspekten der Identität erläutert (kulturelle Identität, Herkunft et cetera). Wichtig ist, dass nicht nur die physische Identität, sondern auch die kulturelle und soziale Identität berücksichtigt wird. Die Suche nach diesen Daten, die in der Regel in jeder Abteilung des Unternehmens auftauchen, ist eine Detektivarbeit. Es sei denn, die Daten liegen bereits systematisch aufbereitet im IT-System vor. In diesem Prozess sind auch die Fragen zu beantworten, in welchem Zusammenhang die personenbezogenen Daten erfasst und verwendet wurden. Beispielsweise welche Rechtsgrundlagen und Erlaubnisse damit verbunden sind.

Beim Thema Informationspflicht wird unterschieden zwischen der Erhebung personenbezogener Daten bei dem Betroffenen selbst und den Pflichten, wenn die Aufnahme nicht direkt bei dem Betroffenen erfolgte. Grundsatz ist die Transparenz im Sinne von „Wer, was, wann bei welcher Gelegenheit über eine Person weiß". Konkret geht es gegenüber Betroffenen um die Benennung eines Verantwortlichen, um Informationen über den Zweck, um die Interessen und die Rechtsgrundlage, sowie die Nennung des Empfängers. Beruht die Verarbeitung der Informationen auf einer Einwilligung, muss der im Unternehmen Verantwortliche nachweisen können, dass eine Zustimmung der Betroffenen vorliegt.

Maßnahmen und Ereignisse müssen dokumentiert und jederzeit nachvollziehbar sein. Bei Datenschutzvorfällen sind diese unverzüglich der Datenschutzaufsichtsbehörde zu melden, sofern der Schutz personenbezogener Daten verletzt wurde. Im Rahmen der EU-DSGVO ist für eine Datenschutz-Folgenabschätzung zu sorgen. Es geht um die Risikoeinschätzung, die ein datenverarbeitendes Unternehmen vor der Verarbeitung personenbezogener Daten vornehmen muss.

Elektronische Kommunikation wird effizienter und sicherer

In Ergänzung zur EU-DSGVO wird an einer „ePrivacy-Verordnung" gearbeitet. Da die EU-DSGVO nur generell die persönlichen Daten der Verbraucher und Internetnutzer innerhalb der EU schützt, wird das Datenschutzrecht für die weltweite elektronische Kommunikation reformiert. Sie knüpft an die Regelungen der Datenschutzgrundverordnung an und postuliert die Voraussetzungen für elektronische Kommunikation. Konsequenz: Wer künftig einen Cookie setzen will, braucht das ausdrückliche Einverständnis des Nutzers.

Erwartungsgemäß finden sich in vielen Artikeln der EU-Datenschutz-Grundverordnung Aufgaben von Datensicherheit im Allgemeinen und im Speziellen. Sicherheit ist eine übergeordnete Instanz für die Funktion des Gesamtsystems. Der Wirksamkeit von Datenschutz-Kontrollen fällt in der Checkliste eine große Bedeutung zu.

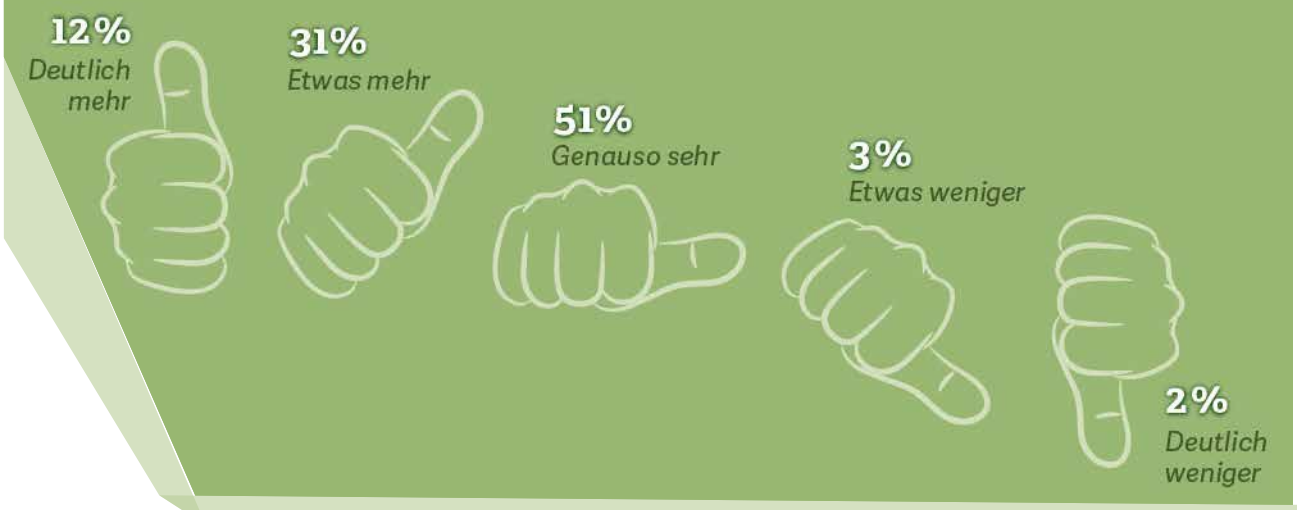
Konkrete Hinweise enthält die EU-DSGVO zur Pseudonymisierung personenbezogener Daten und zu den geeigneten Methoden der Verschlüsselung. Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und die Verfügbarkeit der personenbezogenen Daten und der Verarbeitungssysteme werden definiert. In regelmäßigen Intervallen werden zur Wiederherstellung von Daten und Systemen Zeiten festgelegt.

Alles in allem wird die EU-DSGVO die Unternehmens-IT fordern. Aber am Ende wird ein Datenschutz geschaffen, der diesen Begriff verdient. Die Vorfreude auf den Monat Mai dürfte bereits jetzt Frühlingsgefühle bei Verbrauchern erzeugen. ●

Umfrage zum Vertrauen in den Datenschutz bei deutschen Unternehmen 2017

Haben Sie bei deutschen Unternehmen (zum Beispiel Otto, Xing) mehr Vertrauen in die Datensicherheit als bei amerikanischen (zum Beispiel Amazon, Facebook)?

Deutschen Unternehmen vertraue ich …



Quelle: Statista-Umfrage, 2017

WERBEBEITRAG | UNTERNEHMENSPORTRÄT

EU-DSGVO-konform mit IT-Sicherheit

Laut Gartner werden mehr als die Hälfte aller betroffenen Unternehmen die EU-DSGVO-Richtlinien bis Ende 2018 nicht umgesetzt haben. Dabei müssen sich Unternehmen in der EU, die personenbezogene Daten speichern oder verarbeiten, bis zum 25. Mai 2018 an die neue Rechtslage anpassen, sonst drohen hohe Bußgelder. G DATA zeigt Unternehmen, wie sie mit ganzheitlicher IT-Sicherheit EU-DSGVO-konform werden.

Aber welche Maßnahmen müssen konkret ergriffen werden? Dragomir Vatkov, Head of Product Management bei der G DATA Software AG, stellt klar: „Konformität zur EU-DSGVO entsteht grundsätzlich auf einem strategischen und organisatorischen Level, durch Dokumentation und Prozessoptimierung". Unternehmen müssen einen Datenschutzbeauftragten benennen, mögliche Brennpunkte bei der Umsetzung der EU-DSGVO identifizieren, die eigenen Workflows prüfen und vor allem die IT-Infrastruktur absichern.

Die G DATA Software AG aus Deutschland bietet mit dem Layered-Security-Konzept ganzheitliche IT-Sicherheitslösungen, die Unternehmen einen EU-DSGVO-konformen Betrieb ermöglichen. Mit Policy Management, Mobile Device Management und Network Monitoring hat das Unternehmen unverzichtbare Werkzeuge für die effektive und effiziente Umsetzung der Compliance-Richtlinien im Portfolio. Auf Wunsch erstellen die Experten der G DATA Advanced Analytics gemeinsam mit Unternehmen maßgeschneiderte IT-Compliance-Richtlinien.

G DATA bietet Lösungen und Dienstleistungen, die einen EU-DSGVO-konformen Betrieb ermöglichen.

Die G DATA Software AG bietet am 27.02.2018, zwischen 10:00 und 11:00 Uhr das kostenlose Webinar „EU-DSGVO-konform mit ganzheitlicher IT-Sicherheit" an. Erfahren Sie wie G DATA Software AG bei der Einhaltung der EU-DSGVO unterstützt und melden Sie sich ganz einfach direkt an:

secure.gd/webinar

WERBEBEITRAG | UNTERNEHMENSPORTRÄT

EU-DSGVO Umsetzung – Was kann ich jetzt noch tun?

Am 25. Mai 2018 werden die EU-Datenschutz-Grundverordnung (EU-DSGVO) und das neue Bundesdatenschutzgesetz (BDSG) unmittelbar wirksam. Bis dahin verbleiben nur noch wenige Wochen. Was Unternehmen jetzt noch tun können, erklärt Barbara Scheben, Partner bei KPMG.

„Wer noch am Anfang steht muss nun die Weichen richtig stellen". Barbara Scheben, Rechtsanwältin, Partner, KPMG AG Wirtschaftsprüfungsgesellschaft

Die Umsetzung der EU-DSGVO ist ein komplexes Unterfangen. Sie zielt auf die Einrichtung eines Datenschutz-Management-Systems (DSMS) ab. Proaktivität, Regelkreisläufe und Dokumentation stehen im Vordergrund. Dies ist oft neu, war doch der Datenschutz, so die Erfahrung aus der Praxis, bislang eher reaktiv ausgestaltet. Viele Unternehmen haben bereits Umsetzungsprojekte gestartet und werden zum 25. Mai 2018 einen soliden Stand der Aktivitäten vorweisen können. Es zeigt sich aber auch, dass ebenso viele Unternehmen noch am Anfang stehen. Was nun zählt, sind die richtigen Weichenstellungen zur Einleitung der wesentlichen Maßnahmen.

Anwendungsbereich und Verarbeitungsverzeichnis

Das künftige DSMS muss das Unternehmen als Ganzes umfassen, zum Beispiel auch Tochtergesellschaften und Auslandsniederlassungen. Bemessungsgrundlage für ein mögliches Bußgeld sind bis zu vier Prozent des „gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres". Es sind also nicht nur Compliance-Erwägungen, sondern auch Risikoerwägungen ausschlaggebend. Die Umsetzung hat auch Gesellschaften außerhalb der EU zu umfassen, soweit sich deren Waren oder Dienstleistungen an EU Bürger richten oder deren Verhalten in der EU beobachtet wird. Das Shared-Service-Center in Indien, die Produktion in Südamerika, die Tochtergesellschaft in Afrika können betroffen sein. Neben der EU-DSGVO ist die Umsetzung der Öffnungsklauseln in den EU Mitgliedstaaten einzukalkulieren; in Deutschland zum Beispiel das neue BDSG.

EU-Datenschutzgrundverordnung: Die Zeit läuft!

Dreh- und Angelpunkt des DSMS wird das Verarbeitungsverzeichnis, welches ein Unternehmen sowohl als datenschutzrechtlich „Verantwortlicher" als auch als Auftragsverarbeiter zu führen hat. Es dient im Sinne der Rechenschaftspflicht als Basis-Dokumentation. Das Verarbeitungsverzeichnis geht weit über das bisher bekannte „öffentliche Verfahrensverzeichnis" oder eine Auflistung aller IT-Systeme hinaus. Es setzt auf den Geschäftsprozessen auf und dokumentiert zum Beispiel die Zwecke der Verarbeitung, die Kategorien betroffener Personen und Daten, die Empfänger der Daten, die Fristen zur Löschung wie auch die technisch-organisatorischen Maßnahmen zu ihrem Schutz. Idealer Weise erfolgt zudem eine Zuordnung der Rechtsgrundlagen sowie der eingesetzten Systeme und Anwendungen.

Risikoanalysen, Betroffenenrechte und Drittbeziehungen

Hierauf aufsetzend sind solche Datenverarbeitungen, die ein hohes Risiko für die Betroffenen bergen, einer Datenschutz-Folgenabschätzung zu unterziehen. Bis zum 25. Mai. sollten diese Analysen priorisiert und entsprechende Maßnahmen zur Datensicherheit eingerichtet werden. Mit Blick auf die Datenschutzorganisation sollten vor allem die Prozesse zur Sicherstellung der Betroffenenrechte wie auch zur Meldung von Datenschutzverstößen zum Stichtag konzipiert sein. Wichtig ist zudem die Verwendung angepasster Vorlagen zur Einwilligung und Information.

Dienstleisterbeziehungen als Auftraggeber, Joint Controller oder Auftragnehmer wie auch – ein Klassiker – im Rahmen des konzerninternen Datenaustauschs sind zu klären. Die Frage nach dem „Wer bin ich" stellt Unternehmen oft vor Herausforderungen. Sehr komplex wird das Thema Löschen von Daten. Wer sich hierzu noch keine Gedanken gemacht hat, sollte spätestens jetzt in die Konzeption einsteigen, wenn auch eine Finalisierung in den verbleibenden Wochen weitestgehend unmöglich sein wird.

Der vorgenannte Überblick ist nicht abschließend; die EU-DSGVO stellt zahlreiche Anforderungen. Die ersten Schritte müssen aber getan werden, um die künftige Datenschutzorganisation auch über den 25. Mai 2018 hinaus der EU-DSGVO entsprechend aufzustellen. Der Konzeptions- und Umsetzungsphase werden Prüfungen des DSMS, seien sie extern oder intern, folgen. Insoweit gilt: der Weg ist das Ziel.

www.kpmg.com

Die Zeit wird knapp – worauf es jetzt ankommt.

FOKUSINTERVIEW

„Cybersicherheit zuerst"

Die Digitalisierung von Wirtschaft und Behörden muss mit IT-Sicherheit einhergehen. Dr. Holger Mühlbauer, Geschäftsführer des Bundesverbandes IT-Sicherheit TeleTrusT, fordert konkrete Maßnahmen für die Erhöhung des Sicherheitsniveaus.

Welche Schritte wären jetzt wichtig? Die regierungsbildenden Parteien müssen ein jährliches Budget von mindestens einer Milliarde Euro für die Stärkung der Cybersicherheit von Behörden und Wirtschaft in den Koalitionsvertrag aufnehmen, um dringend erforderliche finanzielle und organisatorische Maßnahmen umzusetzen, die das Cybersicherheitsniveau in Unternehmen und Behörden deutlich erhöhen.

Warum steckt in nachhaltiger IT-Sicherheit der Schlüssel für den Erfolg digitaler Transformation? Der digitale Standort Deutschland wird damit nachhaltig attraktiver, auch für ausländische Investoren. Investitionen in Cybersicherheit wirken flächendeckend auf die Verfügbarkeit aller digital vernetzten Infrastrukturen. Die neue Bundesregierung hat die Chance, die eigene IT-Sicherheitswirtschaft zu stärken und europäische und internationale Kooperationsprojekte aufzubauen.

Welche konkreten Maßnahmen sollten schnell und gezielt umgesetzt werden? Neue Anreizsyseme für den Ausbau von IT-Sicherheitsmaßnahmen nach dem Stand der Technik, Entwicklung neuer Basis-Sicherheitsprodukte, Programme für Wirtschaft und Behörden, um Cybersicherheits-Lösungen „made in Germany" einzuführen, Investitionen in Kooperationprogramme zwischen Anwendern und Industrie, Usability- und Betriebsanforderungen von IT-Architekturen an den Bedürfnissen des Mittelstandes ausrichten.

IT-SICHERHEIT UND DATENTRANSFER

Limits auf dem elektronischen Highway

Von Karl-Heinz Möller

Täglich stehen in Unternehmen Fragen zur Sicherheit von Daten zur Debatte. Verwunderlich ist das nicht, lagern und strömen doch nahezu alle bedeutenden Informationen in einem System von digitalen Netzen und Milliarden von Rechnern. Die Daten und deren Verkehr zu schützen und zu sichern, ist existenziell. Diese komplexen Beziehungen und Zusammenhänge werden aktuell europaweit neu geregelt.

Datensicherheit ist ein essenzieller Bestandteil des lokalen und globalen Managements. Einerseits gelten Informationen heute als der größte Schatz von Unternehmen, siehe Google, Amazon oder Facebook, aber auch Zalando, Otto oder Deutsche Telekom. Andrerseits gehören die Daten den Personen, die sie selbst beschreiben und deren Urheber sie per se sind. Sie unterliegen daher einem besonderen Schutz. Datensicherheit im weiteren Sinne dient vor allem der Vermeidung und Bekämpfung von Cyberkriminalität.

Im Unternehmen gehören zu den organisatorischen Maßnahmen der Datensicherheit unter anderem das regelmäßige Erstellen von Backups, deren Aufbewahrung sowie Zugangskontrollen und Verlaufsprotokolle. Im Konzert mit Schutzsoftware gegen Viren und Schädlingsprogrammen richten sich diese Maßnahmen gegen den virtuellen Datenverlust.

Anzeigepflicht bei Datenschutzverletzungen

Personenbezogene Daten in Unternehmen müssen künftig im Rahmen der neuen Verordnung unter neuen Gesichtspunkten gesammelt und gespeichert werden. Darüber hinaus sind Unternehmen aufgefordert, strengere Auflagen und Bedingungen bezüglich deren Nutzung zu erfüllen. Bei Einzelpersonen bedarf es nach EU-DSGVO einer ausdrücklichen Zustimmung. Wobei ein Einverständnis so deutlich formuliert sein muss, dass der Verwendungszweck klar hervorgeht. Die Genehmigung kann jederzeit widerrufen werden.

Die fachliche Hoheit und Verantwortung für die Sicherheit trägt ein eigens dafür bestimmter Datenschutzbeauftragter (DSB). In Verwaltungen, Behörden und Unternehmen sind diese Mitarbeiter dafür ausgebildet, speziell personenbezogene Daten umfassend zu schützen und entsprechend zu betreuen. Die Datenschutzbeauftragten müssen bei einem Verstoß alle relevanten Aufsichtsbehörden ohne „unangemessene Verzögerung“ und soweit möglich unterrichten. Der Zeitraum in dem die Datenschutzverletzung angezeigt werden muss beträgt 72 Stunden nach erster Kenntnisnahme. Nur wenn die Verletzung keine Folgen für die Rechte und Freiheiten von betroffenen Einzelpersonen hat, kann von dieser Meldung abgesehen werden. Alle Einzelpersonen, die eine Verletzung der Privatsphäre erlitten haben, müssen ebenfalls umgehend informiert werden.

Fragmentierung der Daten muss gesetzeskonform gelöst werden

Der Datenschutz gilt seit langem als das größte Hemmnis, wenn es bei Unternehmen in Deutschland um die Entscheidung für Cloud-Computing geht. Trotzdem steigt die betriebliche Cloud-Nutzung in Deutschland weiter an, wie der Cloud Monitor 2017 von Bitkom Research zeigt. Die Mehrheit der IT-Entscheider hält die Cloud für entsprechend sicher: Nach den Ergebnissen der Bitkom-Umfrage halten 57 Prozent ihre Unternehmensdaten in der Public Cloud für „sehr sicher“ oder „eher sicher“. Nur vier Prozent halten ihre Daten für „sehr unsicher“ oder „eher unsicher“. 37 Prozent können keine klare Aussage machen.

Verschlüsselung auf allen Plattformen

Die ab dem 25. Mai anzuwendende Datenschutz-Grundverordnung könnte die Unsicherheit bei den IT-Managern noch verstärken: Der Veritas 2017 GDPR Report ergab, dass sich fast die Hälfte (48 Prozent) der befragten deutschen Unternehmen noch in der Mitte des vergangenen Jahres nicht gerüstet fühlt für die EU-DSGVO. Die Fragmentierung von Daten und der fehlende Einblick in die Daten seien die größten Herausforderungen. IT-Fachleute gehen dennoch nicht davon aus, dass die Unsicherheit das Cloud-Wachstum spürbar bremsen. Bereits bestehende Datenschutzbedenken hätten dem Cloud-Boom bisher keinen Abbruch getan.

In einer lückenlosen Verschlüsselung steckt auch hier die Lösung. Viele Programme arbeiten nur auf einer bestimmten Plattform, zum Beispiel auf einem Windows-PC, auf einem Android-Smartphone oder in einer bestimmten Cloud. Sind Dateien auf dem Desktop-PC verschlüsselt, muss das auf mobilen Endgeräten ebenso der Fall sein. Sogenannte Always-on-Dateiverschlüsselungen übernehmen Daten von allen mobilen Geräten, Laptops, Desktop-PCs, lokalen Netzwerken und Cloud-basierten File-Sharing-Anwendungen. Spätestens das Inkrafttreten des Gesetzes im Mai dürfte für genügend Überzeugungskraft sorgen, umfassende Sicherheitsmaßnahmen zu installieren. ●

Rechte der Betroffenen

Die drei wichtigsten Rechte sind Selbstbestimmung, Auskunftsanspruch und Löschung der Daten.

- Jede Person muss der Speicherung und Verarbeitung seiner Daten zu einem bestimmten Zweck zustimmen. Mit Inkrafttreten der DSGVO 2018 genügt nicht mehr stillschweigendes Einverständnis. Der Betroffene muss aktive Zustimmung geben.
- Den Betroffenen steht ein Auskunftsrecht zu.
- Die Berichtigung, Löschung und Sperrung der Daten ist jederzeit möglich.

Falsche, veraltete, widerrechtlich gespeicherte personenbezogene Daten müssen von den Datensammlern rechtzeitig gesperrt, berichtigt oder gelöscht werden.

IT-SICHERHEIT UND PRÄVENTION

Volle Transparenz im Netz

Von Karl-Heinz Möller

Bei der Diskussion um Sicherheit sind zu unterscheiden die Daten der Privatsphäre und die in der Interaktion mit Unternehmen und Behörden entstehenden Informationen. Im Fokus der Datensicherheit stehen nicht nur der Schutz der Daten vor Verlust, Verfälschung, Beschädigung, Kopie, Missbrauch und Löschung durch organisatorische und technische Maßnahmen. Im engeren Sinne gehören die stillschweigende und ungeregelte Weitergabe und Nutzung persönlicher Informationen ebenso dazu.

Dank vereinheitlichter Regeln im Umgang mit personenbezogenen Daten durch private Unternehmen und öffentliche Stellen gelten zukünftig europaweit schärfere Bedingungen. Konkret geht es insbesondere um die Wahrung von Rechten der Betroffenen und den Pflichten der Verantwortlichen. Zu den relevanten Neuerungen gehören beispielsweise das Recht auf Datenmitnahme beziehungsweise Datenportabilität.

Neu ist auch die Maßgabe eines Software-Designs, bei dem Privatsphäre-Einstellungen mit Auslieferung in Anwendungen und Produkten voreingestellt sind. Mit der Datenschutzfolgeabschätzung sollen Risiken einer Datenverarbeitung und deren möglicher Folgen für die persönlichen Rechte und Freiheiten der Betroffenen künftig vorab beurteilt werden können.

Weiterhin ermutigt die EU-DSGVO zur Entwicklung sogenannter Verfahrensregeln (Code of Conduct), um die oft abstrakten Vorgaben für den eigenen Geschäftsbereich zu konkretisieren. Das Verhältnis von Datenschutz und IT-Sicherheit wird ausdrücklich definiert. Unternehmen werden verpflichtet, IT-Sicherheitsmaßnahmen unter Berücksichtigung des aktuellen Standes der Technik zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Prävention schützt vor Datenverlusten

Mit der Verordnung einher geht die Forderung, dass Unternehmen besonders personenbezogene Daten besser abschirmen. Ein wichtiger Schritt, solche Daten besser zu schützen, ist das Monitoring aller Vorgänge im gesamten Netzwerk. Zum einen, um Sicherheitsvorfälle durch Angriffe aufzudecken, aber auch um den Abfluss von Daten sowohl extern als auch intern zu vermeiden. In diesem Zusammenhang spielen SIEM-Lösungen (Security Information and Event Management) eine besondere Rolle.

> *Unternehmen werden verpflichtet, Maßnahmen nach aktuellem Stand der Technik zu ergreifen.*

Die Fülle der Angebote von Lösungen für SIEM macht es schwer, eindeutig zu erkennen, was sich hinter dem Begriff wirklich verbirgt. Häufig werden die Anforderungen auf Log-Management und die Analyse von Log-Files (Dateien, die unter anderem Webnutzungen und Adressen dokumentieren) reduziert. Geeignete Lösungen können Events und Log-Files sammeln, korrelieren und analysieren und Sicherheitsvorfälle in Echtzeit analysieren, sowie Reports automatisch erstellen und nicht zuletzt einfach und schnell in bestehende IT-Systeme integriert werden. Bei Cyberangriffen, die auf den Diebstahl personenbezogener Datensätze abzielen, machen diese Systeme sichtbar, was im Netzwerk vorgeht. Per Warnung wird ein tatsächlicher oder versuchter Zugriff auf sensible Bereiche des Firmennetzwerks angezeigt.

Prozesse müssen nahtlos ineinandergreifen

Unternehmen mit großen Datenaufkommen gelingt mit System, tägliche Vorhersagen über ihr Datenaufkommen, Sicherheitsvorfälle und drohende Engpässe zu erhalten. Wenn alle internen Prozesse nahtlos ineinandergreifen, können Mitarbeiter komfortabel in Echtzeit auf gewünschte Daten zugreifen. Besonders aussagefähige Informationen sind aus den Log-Daten zu gewinnen, und eine kontinuierliche und automatisierte Auswertung erfolgt.

Organisationen, die personenbezogene Daten verarbeiten, müssen bis Mai ihre Strategien in die Praxis umgesetzt haben, um ihre IT-Systeme vor Cyberangriffen zu schützen Der Weg zu einem ehrlichen Datencheck könnte über die Simulation einer Attacke erfolgen. Sicherheitsexperten schlüpfen in die Rolle des Hackers und sammeln alle relevanten Informationen für einen Angriff. Nach der Identifikation von Sicherheitslücken wird in Form einer Schwachstellen-Analyse ein Konzept erarbeitet, um mögliche Lücken zu schließen. Eine solche IT-Gesamtaufnahme umfasst die Infrastruktur, die Anwendungen im Internet, die mobilen Geräte, die WLAN-Verbindungen, die zentralen Hardware-Komponenten und alle Web-Applikationen. Werden solche Tests regelmäßig durchgeführt, ist ein relativ hohes Niveau an Vorkehrungen erreicht. Die totale Sicherheit gibt es sowieso nicht. ●

Unternehmen vor Datenklau rechtzeitig schützen

FINANZ- UND FORDERUNGS-IT

Vorfahrt im elektronischen Datenverkehr

Geo-Targeting auf der Basis von Big Data und Data-Mining sowie die Personalisierung der Daten haben in der jüngsten Vergangenheit zu vielen Vorteilen aber auch erheblicher Kritik geführt. Mittlerweile setzt ein Umdenken ein. Es wird angestrebt, den Umfang der erhobenen Daten auf ein Minimum zu reduzieren. Besonders im Finanz-, Versicherungs- und Forderungsbereich sollen bis auf die wirklich relevanten Datensätze keine weiteren Informationen gesammelt, verarbeitet und gespeichert werden. Sicherheit und Schutz der Daten gehen vor.

Von Karl-Heinz Möller

Die neuen regulativen Anforderungen und strengen Regeln für den Schutz personenbezogener Daten sorgen im digitalisierten Finanz- und Versicherungsgeschäft für Handlungsdruck. Sichere Authentifizierungsmethoden spielen dabei eine entscheidende Rolle. Das klassische Pärchen Benutzername und Passwort hat damit weitgehend ausgedient. Es ist vor allem für Transaktionen und Tätigkeiten mit der sensiblen Ware Geld ein Auslaufmodell und wird von Mehrfaktoren-Authentizität abgelöst.

Nicht nur die wachsende Zahl an Cyberangriffen, sondern auch der hingenommene „Missbrauch" von persönlichen Daten hat zu Initiativen und konkreten Schritten zum Schutz personenbezogener Daten und zur Anpassung des gesetzlichen Rahmens an die zunehmenden kriminellen Aktivitäten geführt.

Elektronisches Bezahlen soll nicht nur sicherer, sondern auch bequemer werden

Als übergeordnete Regelung enthält die EU-Datenschutzgrundverordnung detaillierte Weisungen im Umgang mit personenbezogenen Daten durch Unternehmen und öffentliche Stellen. Zusätzlich wird im Rahmen der Zahlungsrichtlinie (PSD2) der Europäischen Kommission die Sicherheit im elektronischen Zahlungsverkehr erhöht. Eine weitreichende Konsequenz dieser Maßnahme ist das Ende des Monopols der Bankinstitute auf die Kontoinformationen der Kunden.

Insgesamt ist beabsichtigt, das elektronische Bezahlen bequemer und günstiger zu gestalten. Der Prozess eines florierenden digitalen Binnenmarktes soll dabei eher gefördert als gebremst werden.

Dabei konzentriert sich die EU-DSGVO ganz besonders auf den Schutz der Intimsphäre und nicht nur auf den Datenschutz im Allgemeinen. Um Compliance-Richtlinien zu genügen und den Datenschutz in diesem Sinne umzusetzen, werden etliche Unternehmen ihren Anstrengungen auf eine höhere und weitreichendere Ebene heben. Sonst dürfte es kaum möglich sein, persönliche Daten im erforderlichen Maß zu kontrollieren und zu verarbeiten.

Auch künstliche Intelligenz könnte dem Schutz der persönlichen Daten dienen

Ob es Chancen gibt, dass der Gesetzgeber noch Spielräume zu eigener Ausgestaltung des Schutzes personensensible Daten gibt, ist nicht endgültig entschieden. Immerhin stecken in diesen ▶▶▶

WERBEBEITRAG | INTERVIEW

„Digitalisierung braucht Sicherheit"

Stefan Wahle, Vorsitzender der Geschäftsführung der Wolters Kluwer Software und Service GmbH, über Digitalisierung und Datenschutz

Worin sehen Sie die gravierendste Neuerung der EU-DSGVO? Unsere Welt wird zunehmend durch die Digitalisierung bestimmt: Immer mehr Lebens- und Arbeitsbereiche verändern sich durch Automatisierung, Robotik und künstliche Intelligenz. Diesen globalen Trends kann sich letztlich niemand entziehen. Daher ist es so wichtig, dass das Recht auf informationelle Selbstbestimmung unbedingt gewährleistet wird. In diesem Kontext ist die gravierendste Neuerung der EU-DSGVO der verstärkte Schutz der personenbezogenen Daten, der durch hohe Strafandrohungen unterstrichen wird – das ist aus meiner Sicht genau richtig, damit sich die Digitalisierung im Sinne der Nutzer entfalten kann.

Was tun Sie als Softwarehersteller für Steuerberater und Mittelstand, damit die EU-DSGVO für Ihre Kunden nicht zum Hindernis im täglichen Geschäft wird? Wir verstehen uns als Innovator der Branche und erschließen unseren Kunden die Möglichkeiten der Digitalisierung. Damit sie dabei die erhöhten Datenschutzanforderungen effizient erfüllen können, haben wir das „EU-DSGVO-Dashboard" entwickelt. Es bietet den Anwendern unserer Software einen zentralen Zugriffspunkt für alle Fragen zum Schutz der personenbezogenen Daten und komfortable Funktionen etwa für die Identifikation von Daten zur Löschung oder die Beantwortung von Auskunftsersuchen.

www.addison.de

WERBEBEITRAG | PRODUKTPORTRÄT

Personendaten rechtzeitig löschen

Finanzinstitute müssen Daten von Personen zu denen keine Geschäftsbeziehung mehr besteht, nach Ablauf der Aufbewahrungsfrist löschen. Häufig finden die operativen Systeme aber eine Vielzahl relevanter Datensätze nicht oder löschen diese zu spät. Die emagixx GmbH bietet hierfür Lösungen, die noch vor Inkrafttreten der EU-DSGVO greifen.

Eigentlich sorgen operative Bankensysteme durch das Setzen eines Kennzeichens dafür, dass inaktive Personendaten fristgerecht gelöscht werden. In einer Reihe von Fällen greift dieser Automatismus aber nicht. So werden viele inaktive Kunden gar nicht als solche erkannt. Auf familiären Beziehungen beruhende systemische Verknüpfungen von inaktiven mit aktiven Datensätzen verhindern zudem das Setzen des Löschkennzeichens. Außerdem kann das im System vorhandene Löschdatum aufgrund von zum Beispiel migrationsbedingten „Reaktivierungen" zum Teil erheblich vom gesetzlich geforderten abweichen. Zusammengenommen handelt es sich in der Regel um eine Vielzahl von Datensätzen, deren Aufbewahrung gegen die gesetzlichen Vorschriften verstößt.

Schnelle und effektive Abhilfe

emagixx verschafft Finanzinstituten einen Überblick über die Anzahl der betroffenen Datensätze. Mit der Dienstleistung Reorganisation steht zudem eine Möglichkeit zur Verfügung, Problemfälle noch rechtzeitig vor in Kraft treten der EU-DSGVO zu löschen.

Produkte von emagixx ermöglichen sicheres Erkennen und Löschen problematischer Datensätze

www.emagixx.de

▶▶▶ Informationen enorme ökonomische Pfründe. Für viele Verlage beispielsweise gehören die Auswertung und Weitergabe zum Geschäftsmodell. So hoffen deren Marketing-Vorstände immer noch, dass es Auswege gibt, um weiterführende Erkenntnisse aus der Verknüpfung von internen und externen Daten zu schöpfen.

Eine Lösung wäre ein verstärkter technischer Datenschutz, um den Zielkonflikt zwischen Persönlichkeitsschutz und digitalen Innovationen einerseits und Nutzerfreundlichkeit und Intimsphäre zu entspannen. Andere Möglichkeiten stecken in einer geschickt programmierten Verschleierung der Daten, die nur wenig Rückschlüsse auf die sich dahinter verbergenden Personen zuließen.

Auch der Einsatz künstlicher Intelligenz oder mit Kontroll-Algorithmen aufgebaute Programme sind denkbar. Die Phantasie der Juristen war in diesem Punkt wohl nicht ausschweifend. IT-Experten denken auch an eine mit Datenschutzregeln gefütterte und von Datenschützern kontrollierte Software, die über die Einhaltung von Persönlichkeitsrechten wacht. Ganz zu schweigen von den Chancen, die eine Blockchain-Technologie böte. Speicherereignisse könnten in Verzeichnissen vermerkt und auf verschiedene Beteiligte, Rechner und Unternehmen verteilt sein.

Verantwortung im sensiblen Umgang mit Forderungen und Abtretungen wird aufgeteilt

Ein großes Thema im Zahlungsverkehr ist der Umgang mit Forderungen. Werden ausstehende Forderungen übertragen, gelten besondere Regelungen zum Schutz dieser Informationen, je nach Vertragsgestaltung. Tritt ein Gläubiger seine Forderung in Form eines Verkaufs an ein Inkassounternehmen ab, handelt es sich datenschutzrechtlich um den Fall einer Funktionsübertragung. Ein Inkassobüro macht die Forderung im eigenen Namen geltend und handelt nicht weisungsgebunden. Bei diesem Verfahren wählt das Inkassounternehmen die Maßnahmen zur Beitreibung der Forderung eigenverantwortlich.

Die Erhebung und Verarbeitung der Daten durch ein Inkassounternehmen erfolgt in diesem Fall für eigene Geschäftszwecke und unterliegt somit den Vorschriften des Bundesdatenschutzgesetzes (BDSG). Der Gläubiger kann sich bezüglich der Übermittlung der Daten an das Inkassounternehmen ebenfalls auf diese Regelung berufen. Die Begleichung der Forderung kann als berechtigtes Interesse des übermittelnden Unternehmens angesehen werden.

Die Vorschrift greift so lange, wie kein schutzwürdiges Interesse des Schuldners überwiegt. Vorsicht sei nach Ansicht von Rechtsexperten beispielsweise dann geboten, wenn das beauftragte Inkassounternehmen gleichzeitig als Auskunftei tätig ist. Das Inkassounternehmen darf die ihm zum Zwecke des Forderungseinzugs übermittelten Daten ausschließlich dafür verwenden. Die Informationen dürfen keinesfalls in die Tätigkeit als Auskunftei mit einfließen.

Persönliche Daten müssen beim Kauf geschützt bleiben

Bei Forderungseinzug liegt eine Datenverarbeitung im Auftrag vor. Zu den lediglich unterstützenden Tätigkeiten können die Erstellung von Mahnungen, Feststellung der aktuellen Anschrift oder Überwachung des Zahlungseingangs gehören.

Eine wichtige Neuerung für Kunden ist das Recht auf Löschung gemäß EU-DSGVO. Die betroffene Person kann von dem Verantwortlichen verlangen, dass die personenbezogenen Daten unverzüglich gelöscht werden, vor allem, wenn die Daten für den vorgesehenen Zweck nicht mehr notwendig sind. Das klingt nach echtem Verbraucherschutz. ●

Missbrauch im Datenschutz

In der Praxis häufig verletzte Normen und Verstöße:

- Es wurde kein Datenschutzbeauftragter in der vorgeschriebenen Form bestellt.
- Bußgelder, wenn ein Auftrag im Rahmen der Auftragsdatenverarbeitung nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt wurde.
- Unterlassen der Unterrichtung des Betroffenen bei der Nutzung von Daten für Werbezwecke und für den Adresshandel.
- Verstöße bei der Erteilung einer Auskunft an den Betroffenen. Auskunft wird nicht richtig, vollständig oder rechtzeitig erteilt.

Was Sie über die EU-DSGVO wissen müssen

Die gute Nachricht vorab: Jedes Unternehmen, das den Datenschutz schon bisher ernst genommen hat, seine Prozesse dokumentiert und einen Datenschutzbeauftragten hat, ist gut auf den bevorstehenden Geltungstags der EU-Datenschutzgrundverordnung (EU-DSGVO) am 25. Mai 2018 vorbereitet. Arvato Financial Solutions gibt hier einen Überblick über die wichtigsten Änderungen und berät Sie gerne.

Die EU-DSGVO soll mit der Harmonisierung des Datenschutzes EU-weit gleiche Wettbewerbsbedingungen für Unternehmen schaffen. Ziel ist es, alle EU-Bürger in einer datengetriebenen Welt vor Datenschutzverstößen zu schützen.

Die größte Veränderung betrifft den erweiterten Geltungsbereich. Er erstreckt sich auf alle Unternehmen, die Daten von EU-Bürgern verarbeiten, und zwar ungeachtet ihres Firmensitzes. Sogenannte Öffnungsklauseln erlauben den Staaten, Regelungslücken durch nationale Gesetze auszufüllen. In Deutschland wird die Verordnung durch das neue Bundesdatenschutzgesetz ergänzt.

Was sind die wichtigsten Änderungen?

Absehbar ist, dass die neue EU-DSGVO Raum für Interpretation bieten wird im Hinblick darauf, was sie für Unternehmen in den verschiedenen EU-Mitgliedstaaten bedeutet. Die Erhebung und weitere Verarbeitung personenbezogener Daten durch Inkassounternehmen und Auskunfteien ist auf alle Fälle weiterhin legitimiert.

Die EU-DSGVO hält an dem Verbot mit Erlaubnisvorbehalt fest. Danach ist jede Verarbeitung personenbezogener Daten zunächst verboten, soweit nicht eine Einwilligung vorliegt oder eine Erlaubnisnorm greift. So ist eine Datenverarbeitung zur Erfüllung eines Vertrages – dazu gehört auch die Durchsetzung offener Zahlungen – sowie zur Wahrung berechtigter Interessen zulässig.

Einwilligungen sind allerdings nur wirksam, wenn diese „informiert" erfolgen. Das heißt, Verbraucher müssen vorab informiert werden, welche Datenkategorien zu welchen Zwecken gespeichert werden. Das war auch bisher schon so. Aber die Rechte von Verbrauchern werden durch neue Transparenz- und erweiterte Informationspflichten weiter gestärkt. Damit sich der Verbraucher einfach informieren kann, ist es sinnvoll, diese Angaben schon im Bestell- oder Antragsprozess zu hinterlegen.

Sind Sie bereit für die EU-DSGVO?

Welche Sanktionen gibt es?

Die neue Verordnung soll nicht nur wirksam sein, sondern auch abschrecken. Entsprechend hoch sind die Strafen. Bei Verstößen gegen Verbraucherrechte, fehlenden Rechtsgrundlagen für die Verarbeitung der Daten, Anordnungen der Aufsichtsbehörde oder Drittlandübermittlung sind bis zu 20 Millionen Euro oder vier Prozent des weltweiten Vorjahresumsatzes fällig. Außerdem müssen Unternehmen bei gravierenden Datenschutzverstößen die Aufsichtsbehörde binnen 72 Stunden informieren. Da heißt es, schnelle und effiziente Prozesse zu etablieren.

Sie möchten mehr erfahren? Dann laden Sie unser White Paper herunter.

finance.arvato.com/dsgvo

ePRIVACY

Vorprogrammierter Datenschutz

Von Paul Trebol

Wie eine Lambda-Sonde in moderneren Automobilen, die die Abgase reinigt, kann in Software und Hardware der Datenschutz von Hause aus eingebaut sein und einen rechtskonformen und sicheren Datenverkehr gewährleisten. Anwender, die beispielsweise weltweit elektronisch kommunizieren und Waren erwerben und verkaufen, sichern sich damit ab. Diese und andere Regelungen werden separat in einer Datenschutzverordnung für den Datenverkehr im Internet formuliert, der ePrivacy-Verordnung.

Für den Schutz und die Sicherheit der Daten bricht mit der einheitlichen Datenschutzgrundverordnung ein neues Zeitalter in Europa an. Dass damit noch längst nicht alle Aufgaben rund um die digitalen Informationen, beispielsweise im Verkehr via Internet zwischen Unternehmen, Lieferanten, Kunden sowie behördlichen Institutionen, gemacht sind, zeigt die sogenannte ePrivacy-Verordnung.

> *„Verordnung soll Bürgern wieder mehr Transparenz über die im Netz hinterlassene digitale Spur geben.*

Hintergrund: Eine „ePrivacy“ genannte Richtlinie existiert in der EU seit 2002. Sie gibt eine Mindestvorgabe im Bereich des Datenschutzes an. Ergänzt wurde sie 2009 durch die Cookie-Richtlinie, die unter anderem eine Einwilligung und Aufklärung der Nutzer beim Setzen von Cookies auf Webseiten verlangt. Beide Richtlinien ergänzen die europäischen Datenschutzbestimmungen.

Spezielle Schutzzone im internationalen Datenverkehr via Internet

Da sich die elektronische Kommunikation seither dramatisch verändert hat, sind zwangsläufig inhaltliche Anpassungen in der neuen ePrivacy-Verordnung notwendig. Warum das alles nicht in der EU-DSGVO geregelt wird, hat den Grund, dass die EU-DSGVO eine Grundverordnung ist und damit lediglich die Grundsätze regeln soll. Hauptziel der EU-DSGVO ist es, natürliche Personen bei der Verarbeitung personenbezogener Daten zu schützen.

Die ePrivacy-Verordnung hat den speziellen Schutz des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation im Fokus. Auch wenn es an vielen Stellen große Schnittmengen gibt, haben sich die EU-Datenschützer zur einer separaten ePrivacy-Verordnung entschieden, um die „personenbezogenen Daten“ im internationalen elektronischen Datentransfer in einer speziell eingerichteten Zone zu schützen. Zudem gelten EU-Verordnungen im Vergleich zu Richtlinien unmittelbar in allen Mitgliedsländern und müssen nicht in nationales Recht umgesetzt werden, ein Vorteil.

Datensammeln wird erheblich erschwert

Datenschutz kann schon im Design Teil des Konzeptes sein. Beim „Privacy by Design“ sind Datenschutzanforderungen direkt in der Spezifikation von neuen Produkten oder Funktionen berücksichtigt. Produkte mit der Funktion von „Privacy by Default“ müssen im initialen Zustand einen hohen Datenschutz des Kunden gewährleisten


Respekt der Privatsphäre auch im Job

Die Verordnung soll EU-Bürgern in Zukunft wieder mehr Transparenz und Kontrolle über die im Netz hinterlassene digitale Spur geben. Wer künftig einen Cookie setzen will, braucht ab Inkrafttreten der ePrivacy-Verordnung das ausdrückliche Einverständnis des Nutzers. Mit ihr wurde ein weiteres Sanktionsmodell erschaffen, das in Anlehnung an die Datenschutzgrundverordnung für Unternehmen das Risiko empfindlicher Geldbußen bedeutet. Wegen der anhaltend heftigen Diskussion innerhalb der EU steht ihr Inkrafttreten – geplant war ebenfalls im Mai – noch nicht fest. ●

WERBEBEITRAG | INTERVIEW

„Auf der sicheren Seite“

Instant Messaging ist aus dem Geschäftsalltag nicht mehr wegzudenken. Marco Hauprich, Senior Vice President Digital Labs bei der Deutschen Post AG, erklärt im Interview, warum Unternehmen sich nicht mehr zwischen Usability und Sicherheit entscheiden müssen.

Die Deutsche Post hat mit SIMSme Business einen Messenger ausschließlich für den professionellen Einsatz auf den Markt gebracht. Warum sollten Unternehmen SIMSme Business statt WhatsApp einsetzen? Ganz einfach: Weil die Übermittlung vieler dienstlicher Inhalte mit WhatsApp nach einschlägiger Gesetzeslage und spätestens nach Inkrafttreten der EU-DSGVO schlicht unzulässig ist. Von möglichen Risiken für die Unternehmenssicherheit ganz zu schweigen. Mit SIMSme Business können Firmen rechtlich sicher von den Vorteilen der Messenger-Nutzung profitieren.

Was genau sind die Vorteile? Der Messenger macht die interne Kommunikation schneller, effizienter und bequemer. Inhalte des Kundentermins, Arbeitsaufträge an die Mitarbeiter und ein Foto des Flipcharts mit den Meeting-Ergebnissen – das alles geht zügig an die richtige Person, ohne die bei E-Mails üblichen Cc- und Bcc-Verteiler. Außendienstler sind via Messenger jederzeit und an jedem Ort schnell zu erreichen. Und Administratoren haben mit dem Management Cockpit ein intuitives Werkzeug zur Nutzer- und Lizenzverwaltung – auch vom Desktop-Rechner aus.

Was macht Ihre App so sicher? Bei SIMSme Business werden sämtliche Daten mit Ende-zu-Ende-Verschlüsselung geschützt, nach der Zustellung werden sie gelöscht. Hosting und Betrieb erfolgen auf ISO 27001 zertifizierten Servern, die ausschließlich in Deutschland stehen. Der Dienst ist konform mit dem Bundesdatenschutz und der kommenden EU-DSGVO sowie den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Und wer nutzt SIMSme Business bereits? Zu unseren Kunden gehören unter anderem Volkswagen Financial Services sowie der Bayerische Landkreistag. Das Interesse für SIMSme Business geht aber quer durch alle Branchen.

www.sims.me/business

MANAGEMENTSYSTEME

Lücke schließen zwischen Soll und Ist

Von Paul Trebol

Mit dem Inkrafttreten der Verordnung sind die Anforderungen an den Datenschutz deutlich verschärft worden. Die betroffenen Organisationen müssen demnächst entsprechende Umsetzungsmaßnahmen abgeschlossen haben. Im Rahmen eines Datenschutzmanagementsystems werden die Zuständigkeiten, Prozesse und Maßnahmen neu bewertet.

Unternehmen befinden sich aktuell in der Situation, ihre Maßnahmen zum Datenschutz zu überprüfen, mit den neuen Anforderungen abzugleichen und falls erforderlich anzupassen. Als Vorgehensweise bietet sich eine systematische Soll-Ist-Betrachtung an.

Die aktuelle Situation der Datenschutzorganisation nach dem gültigen Bundesdatenschutzgesetz BDSG wird mit dem zukünftig geltenden Soll-Zustand nach EU-DSGVO abgeglichen, auch „GAP-Analyse“ genannt. Die „Lücke“ zwischen Soll und Ist veranschaulicht, was getan werden muss, um die Anforderungen der EU-DSGVO zu erfüllen.

Aufgeteilt in Projektschritte wird ein Fahrplan erstellt

Auf der Grundlage einer Gap-Analyse können Maßnahmen definiert werden, um den Datenschutz-Soll-Zustand nach EU-DSGVO im Unternehmen aufzubauen. Dieser Schritt ist zugleich der umfangreichste. Zwar beinhaltet die EU-DSGVO keine grundlegenden Änderungen des „Datenschutz-Systems“. Dennoch erfordern deutlich gestiegene Anforderungen an die Transparenz und Dokumentation bei der Verarbeitung personenbezogener Daten und insbesondere deren Absicherung konkrete technische und organisatorische Maßnahmen. Auf der Grundlage des Ist-Soll-Abgleichs kann dann auch eine erste Festlegung der Projektschritte für die Umsetzung der EU-DSGVO erfolgen. In der Terminologie der GAP-Analyse bedeutet dies: Überblick erhalten über bereits vorhandene Prozesse und deren Reifegrad, Aufwandsabschätzung für notwendige Maßnahmen, mögliche Integration von EU-DSGVO-Maßnahmen in ein bestehendes Information Security Management System, kreieren einer optimalen Compliance.

Das Datenschutzkonzept für die Umsetzung der EU-DSGVO ist als eine zusammenfassende Dokumentation aller datenschutzrechtlichen Aspekte im Unternehmen zu verstehen. Es umfasst Ziele, Verantwortlichkeiten und Dokumentationspflichten und gehört zu den wichtigsten Strategiepapieren eines Unternehmens.

> *Managementsysteme müssen die individuellen Bedingungen in einem Unternehmen widerspiegeln.*

Hinterlegung eines Datenschutzkonzeptes sorgt für Transparenz

Datenschutzkonzepte helfen, den Rechenschaftspflichten der europäischen Datenschutzgrundverordnung gegenüber den Aufsichtsbehörden gerecht zu werden. Sie dienen außerdem als Grundlage für datenschutzrechtliche Prüfungen, zum Beispiel durch Auftraggeber.

Unternehmen, die personenbezogene Daten verarbeiten, müssen ein Verfahren einrichten, um die Wirksamkeit der Datenschutz- und Datensicherheits-Maßnahmen regelmäßig zu überprüfen, bewerten und evaluieren. Dafür ist ein Datenschutzkonzept die optimale Ausgangsbasis. Ein Datenschutzkonzept sollte gut strukturiert sein, da es sowohl für interne als auch externe Stakeholder verständlich sein sollte. ●

WERBEBEITRAG | PRODUKTPORTRÄT

Datenschutzmanagement ganz einfach online

Projekt 29 stellt mit Privacysoft das Allround-Werkzeug für EU-DSGVO konformes Datenschutzmanagement vor.

Datenschutz und korrektes Datenschutzmanagement sind schon jetzt oftmals Mammutaufgaben. Die kommende EU-Datenschutz-Grundverordnung bringt noch mehr Anforderungen mit sich. Unternehmen und Organisationen haben ab Mai 2018 deutlich erweiterte Pflichten im Datenschutz und dies bei Bußgeldern bis vier Prozent des weltweiten Vorjahresumsatzes.

Seit 1996 im Bereich des Datenschutzes tätig, haben wir mit Privacysoft ein Onlinetool entwickelt, dass Unternehmen jeder Größe bei allen Anforderungen der EU-DSGVO optimal unterstützt. Flexibel, pragmatisch und trotzdem umfassend, unterstützt Privacysoft die tägliche Arbeit von Datenschutz-Verantwortlichen und hilft, optimale Compliance mit allen Datenschutzvorschriften zu gewährleisten. Eine zeitgemäße und intuitive Benutzeroberfläche, die alle Funktionen übersichtlich strukturiert, macht die Bedienung leicht.

Aktuelle Checklisten, Musterverfahren und Vorlagen helfen, die Unternehmensprozesse zu beleuchten und zu bewerten. Schon bei der Erfassung, Kontrolle, Steuerung, Analyse und Optimierung der Arbeitsabläufe aller Datenschutzprozesse entsteht quasi nebenbei eine revisionssichere Dokumentation. Die praxisorientierte Software macht es möglich, beliebige betriebliche oder konzernweite Strukturen darzustellen und zu verwalten. Und all dies ohne Installations- und Wartungsaufwand, in Deutsch und Englisch.

Mit Privacysoft entspannt die EU-DSGVO umsetzen

www.privacysoft.de

FOKUSINTERVIEW

„Geregelte Verfahren implementieren“

Mit Einführung der EU-DSGVO stehen Unternehmen und ihre IT vor spezifischen Anforderungen. Michael Grötsch, Vorstand der Circle Unlimited AG, beschreibt, welche Maßnahmen zeitnah umzusetzen sind.

Umfragen zeigen, dass ein relativ großer Teil der Unternehmen nicht gut auf die EU-DSGVO vorbereitet ist. Wo lauern die Risiken? Auf Unternehmen könnten eine Fülle von Anfragen zu personenbezogenen Daten zukommen, die ihre Verwaltung bei pflichtgemäßer Bearbeitung lahmlegen. Zustimmungen von Speicherung oder Weitergabe müssen innerhalb kurzer Frist regelgerecht von autorisierten Mitarbeitern beantwortet werden.

Bei personenbezogenen Daten haben Kunden ein Recht auf Auskunft und Löschung. Wie können sich Unternehmen vorbereiten? Sie müssen sicherstellen, dass die erforderlichen Schritte in jedem Einzelfall in konkreten Arbeitsabläufen vorbereitet sind. Dies geschieht mit definierten Workflows, um Dokumentationen nach EU-DSGVO zu generieren. Es bedarf eines geordneten Verfahrens, das die Prüfung und Durchführung der Löschung gestaltet.

Welche Anforderungen sind an die Qualität der IT zu stellen, die personenbezogene Daten verarbeitet? IT-Verfahren müssen in jedem Detail darauf ausgerichtet sein, Grundsätze der EU-DSGVO per se zu beinhalten. Gemeint sind Software-Voreinstellungen wie „privacy by design“ und „privacy by default“. Diese Vorgaben müssen spätestens am 25. Mai für jedes neue System eingehalten werden.

COMPLIANCE

Vertraulichkeit und Integrität sichern

Die gesetzlichen Vorschriften zum Datenschutz spielen künftig bei der Ausgestaltung von Compliance-Management-Systemen eine deutlich zentralere Rolle als bislang. Wobei die praktischen Anforderungen gemäß EU-DSGVO komplexer und umfassender sind. Zum tieferen Verständnis und zur Sensibilisierung der Mitarbeiter werden intensive Weiterbildungsmaßnahmen vorgeschrieben.

Von Paul Trebol

Personenbezogene Daten waren schon immer ein kostbares Gut. Nun wird dieser Bedeutung explizit Rechnung getragen und durch eine der digitalisierten Welt angepassten Gesetzgebung besonders geschützt. Für alle Mitarbeiter, die in ihrem Unternehmen mit personenbezogenen Daten – beispielsweise von Kunden, Lieferanten, Kollegen oder Bewerbern – arbeiten, gelten zukünftig die strengen Vorschriften der EU-DSGVO.

Die Vorgaben berühren insbesondere die Verantwortung im Zusammenhang mit der Compliance-Funktion. Unternehmen sind verpflichtet, Betroffene von der Verarbeitung ihrer personenbezogenen Daten umfassend über die Erhebung und Verwendung der Daten zu informieren und Auskunft zu erteilen. Beispielsweise müssen Unternehmen dokumentieren, wie und mit welchen Werkzeugen sie die Vorgaben einhalten, sowie gegebenenfalls dies gegenüber den Aufsichtsbehörden nachweisen können. Die Verordnung enthält Regelungen darüber, wer für die Daten verantwortlich ist, und wie sie zu verarbeiten sind.

Datensparsamkeit ist als Prinzip im Gesetz verankert

Als Verantwortlicher gilt per Definition die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Verantwortlichen haften dafür, dass bei jedem Verarbeitungsvorgang die Vorschriften der Verordnung eingehalten werden und haben dies durch geeignete Maßnahmen zu gewährleisten. Wenn nötig müssen sie den Nachweis dafür erbringen.

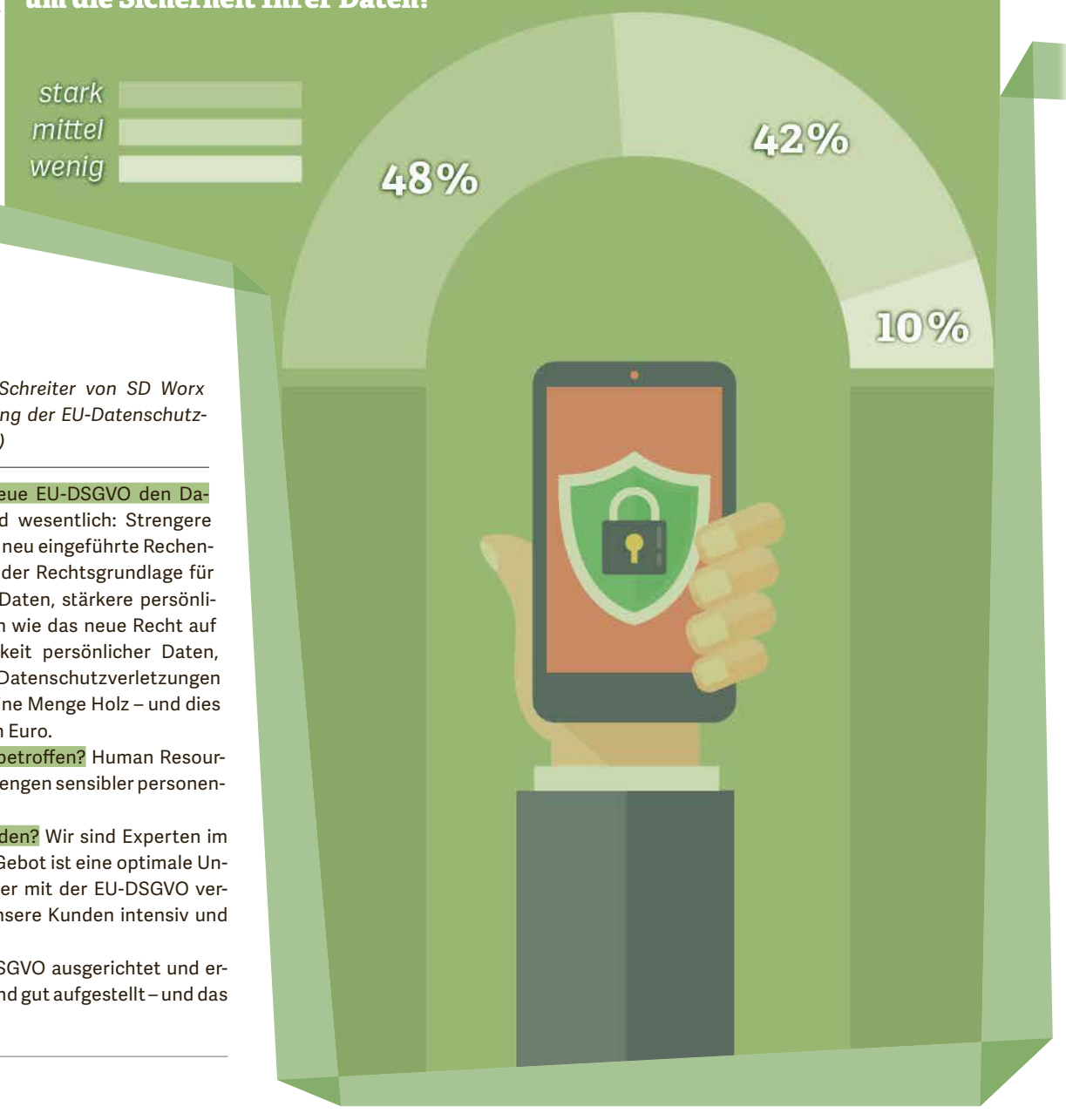
Das bereits im Bundesdatenschutzgesetz BDSG verankerte Prinzip der Datensparsamkeit gilt als eines der zentralen Prinzipien des Datenschutzes. Die Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Die Erlaubnis gilt nur für den einen festgelegten, eindeutigen und legitimen Zweck.

Richtlinien im Umgang mit persönlichen Daten sind zu definieren

Eine sogenannte Datenschutz-Folgenabschätzung wird vorgeschrieben. Diese ist vorzunehmen bei der Verwendung neuer Technologien, falls diese ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnte.

Unternehmen müssen Compliance-Anforderungen nicht nur verstehen, sondern sie müssen sich ganz konkret für den besten Weg, die besten Methoden entscheiden. Dies betrifft sowohl organisatorische Prozesse als auch deren technische Umsetzung. Zu den notwendigen Maßnahmen, die innerhalb der EU-DSGVO festgeschrieben sind, gehört es beispielsweise, die Richtlinien zum Umgang mit sensiblen persönlichen Daten zu definieren und umzusetzen. Um diese Kenntnisse sicherzustellen, sind Schulungen mit entsprechenden Zertifikaten zu organisieren. Gleichzeitig muss es der Sicherheitsansatz eines jeden Unternehmens erlauben, Kompetenz-Prüfungen und Gutachten (Data Protection Impact Assessment DPIA) durchzuführen. ●

Wie sehr sorgen Sie sich bei Social-Media-Unternehmen wie Facebook um die Sicherheit Ihrer Daten?



Quelle: Statista-Umfrage, 2017

WERBEBEITRAG | INTERVIEW

„Mit ruhiger Hand“

Datenschutzexperte Tobias Schreiter von SD Worx über gute Wege zur Umsetzung der EU-Datenschutzgrundverordnung (EU-DSGVO)

Inwieweit verändert die neue EU-DSGVO den Datenschutz? Fünf Punkte sind wesentlich: Strengere Datenschutzpflichten wie die neu eingeführte Rechenschaftspflicht, der Nachweis der Rechtsgrundlage für die Verarbeitung sämtlicher Daten, stärkere persönliche Rechte der Beschäftigten wie das neue Recht auf Löschung oder Übertragbarkeit persönlicher Daten, strengere Meldepflichten bei Datenschutzverletzungen und die Beweislastumkehr in Richtung der Unternehmen. Eine Menge Holz – und dies im Lichte drakonischer neuer Strafen von bis zu 20 Millionen Euro.

Sind auch die Personalabteilungen von der Verordnung betroffen? Human Resources (HR) ist besonders betroffen, denn dort werden große Mengen sensibler personenbezogener Daten verarbeitet.

Wie unterstützt SD Worx als HR-Dienstleister seine Kunden? Wir sind Experten im HR-Umfeld, unsere Kunden vertrauen uns. Unser oberstes Gebot ist eine optimale Unterstützung unserer Kunden bei der Bewältigung sämtlicher mit der EU-DSGVO verbundenen Compliance-Herausforderungen. Wir beraten unsere Kunden intensiv und informieren sie über Neuigkeiten.

Natürlich ist auch unsere Software bereits auf die EU-DSGVO ausgerichtet und erfüllt zuverlässig die genannten neuen Anforderungen. Wir sind gut aufgestellt – und das wissen auch unsere Kunden.

www.sdworx.de/de-de/dsgvo

RECHT

Permanent online mit den Paragraphen

Von Karl-Heinz Möller

Die Einführung neuer Strafvorschriften nach EU-DSGVO bringen im Vergleich zu den bisher gültigen Bedingungen des Bundesdatenschutzgesetzes BDSG erhebliche Schärfungen und empfindlichen Strafzahlungen. Die Beachtung der international geltenden Regeln wird dringend empfohlen. Um die speziellen Strukturen dafür zu schaffen, bleibt gerade noch Zeit bis zum 25. Mai 2018.

Datenschutz war für Unternehmer wie Shop-Betreiber oder Dienstleister schon immer ein äußerst heikles Thema. Kundenbestellungen, Direktwerbung, Mail-Kampagnen oder Nutzertracking: Viele Aktionen glichen einer Gratwanderung und gelten juristisch als ein hochsensibles Betätigungsfeld. Während in Deutschland nach dem aktuellen Bundesdatenschutzgesetz (BDSG) Verstöße mit bis zu 300.000 Euro geahndet wurden, erreicht mit der neuen Datenschutzgrundverordnung das Thema eine neue Dimension. Abgesehen vom wesentlich höheren Aufwand und enormer Komplexität sind in Zukunft Strafzahlungen von bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweit erzielten Jahresumsatzes eines Konzerns möglich.

Dokumentation und Richtlinien zur Folgeabschätzung gehören zum Repertoire

Da sich das Zeitfenster für durchgreifende interne Maßnahmen bald schließt, sollten Punkte geklärt sein, die rechtliche Konsequenzen nach sich ziehen könnten. Konkret bedeutet dies im Einzelnen, dass alle Datenverarbeitungsprozesse, die personenbezogene Daten betreffen, penibel erfasst und dokumentieren sind. Dazu gehören fixierte Richtlinien zur zukünftigen Verarbeitung personenbezogener Daten, damit eine Datenschutz-Folgenabschätzung möglich wird.

Sieben Prinzipien liegen in rechtlicher Betrachtung der Verordnung zugrunde: „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“, „Datenminimierung”, „Richtigkeit“, „Speicherbegrenzung”, „Integrität und Vertraulichkeit“ und „Rechenschaftspflicht“. Demnach müssen personenbezogene Daten sachlich richtig und rechtlich auf dem neuesten Stand sein. Angemessene Maßnahmen sind darüber hinaus zu treffen, falls sie im Zusammenhang ihrer Verarbeitung falsch gespeichert wurden. Speicherbegrenzung bedeutet, dass personenbezogene Daten nur in einer Form gespeichert werden, die für die Identifizierung der betroffenen Personen erforderlich sind. Es sei denn, die Speicherung liegt im öffentlichen Interesse und ist für Archivzwecke oder für wissenschaftliche und historische Forschungungen oder für statistische Analysen wichtig.

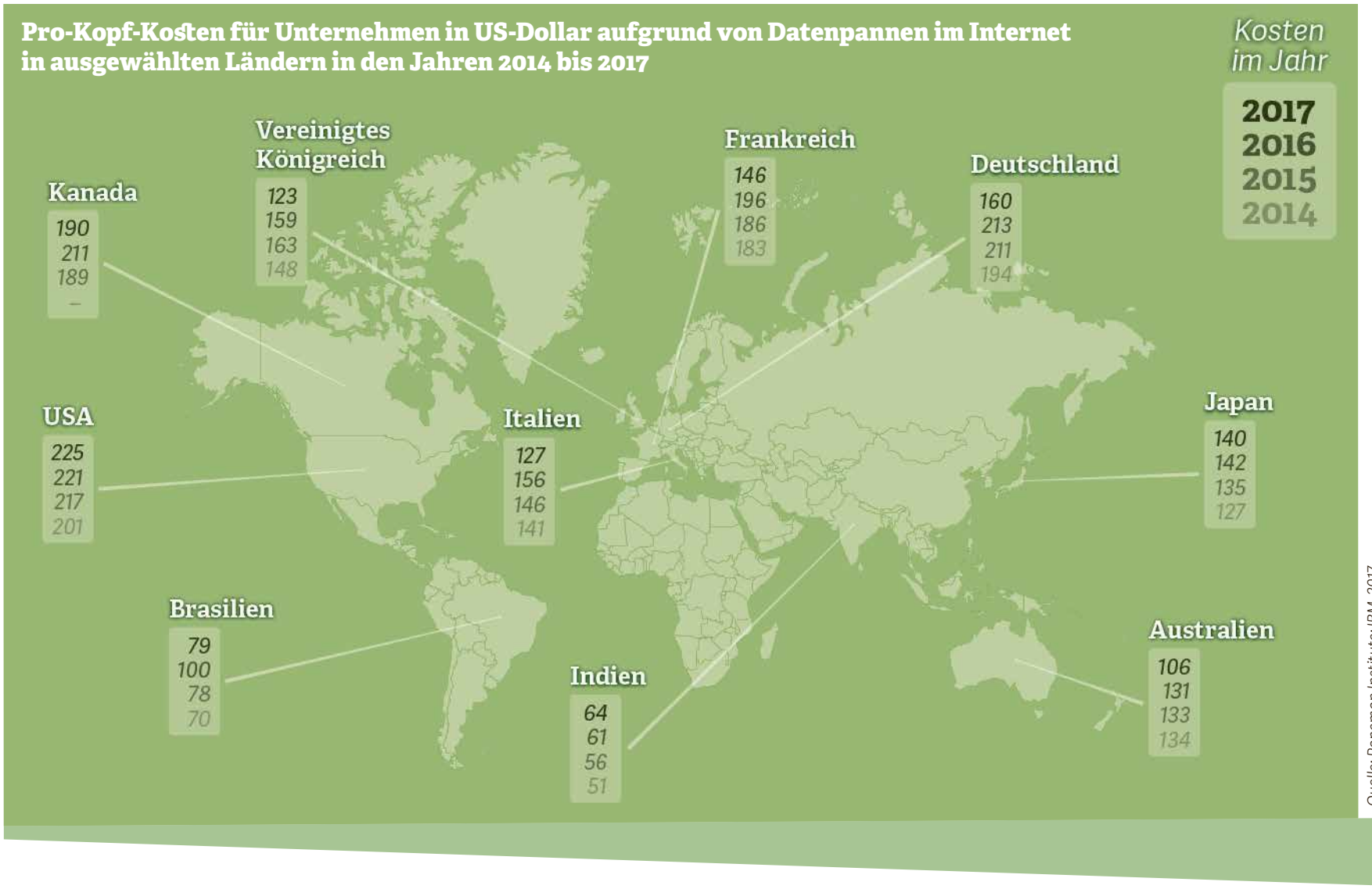
Im Detail unterscheidet die EU-DSGVO in Daten, die beim Betroffenen erhoben werden und Daten, die anderweitig erhoben wurden. Webseitenbetreiber müssen die Verarbeitungszwecke und deren Rechtsgrundlage benennen.

Wenn eine Übermittlung personenbezogener Daten an Dritte beabsichtigt ist, sind die konkreten Empfänger anzugeben. Werden die Daten bei Betroffenen erhoben, müssen sie darauf hingewiesen werden, ob die Bereitstellung für einen Vertragsschluss erforderlich ist.

Für international operierende Händler gilt die Methode des One-Stop-Shop

Weitere Informationspflichten betreffen die Speicherdauer, Betroffenenrechte wie Zugang, Berichtigung, Sperrung, Löschung, Widerspruch und Datenübertragbarkeit. So ist auch das Zugriffsrecht als Ergänzung zum Auskunftsrecht anders als bisher geregelt.

Mit der Datenschutzgrundverordnung wird das Verfahren rund um Datenschutzverstöße und Streitigkeiten vereinfacht. International operierenden Online-Händlern, ist bereits die Methode des One-Stop-Shop vertraut. Sie ermöglicht den EU-Bürgern, dass sie sich bei Beschwerden immer an ihre eigene Datenschutzbehörde wenden können. ●



Quelle: Ponemon Institute; IBM, 2017

GASTBEITRAG

EU-Datenschutzrecht startet im Mai

Jetzt Maßnahmen einleiten!

Das EU-Datenschutzrecht wird zu EU-weit geltenden und weltweit wirkenden Datenschutzstandard mahnt der BvD e. V.

Wichtiger Treiber des neuen Datenschutzrechts ist die Gestaltung der Bußgelder. Mit bis zu vier Prozent des Vorjahresumsatzes eines Unternehmens steigen die möglichen Bußgelder erheblich an. Hinzu kommt, dass die Anzahl der Bußgeldtatbestände erheblich gestiegen ist.

Was Unternehmen nun tun sollten:

1. Datenschutzgrundsätze der EU-DSGVO in das interne Regelwerk integrieren. Richtlinien und Prozesse definieren, Schulungsmaßnahmen dazu durchführen.
2. Dokumentation überprüfen/anpassen – aus dem Verfahrensverzeichnis wird die Verarbeitungsübersicht, die zukünftig im Mittelpunkt des Datenschutzmanagements steht. Rechtsgrundlagen für die Verarbeitungen definieren.
3. Verträge mit Dienstleistern überprüfen und anpassen. Keine Auftragsverarbeitung ohne den entsprechende Vertrag.
4. Betroffenen-Rechte und Informationspflichten gewährleisten und entsprechende Prozesse installieren.
5. Meldepflichten im Unternehmen installieren und Prozesse einrichten, die die jeweilige Meldung fristgerecht ermöglichen.

Die EU-DSGVO richtet sich eindeutig an die Leitung der Verantwortlichen Stelle. Diese ist Adressat der Regelungen, Pflichten und der Haftung. Für viele Unternehmen wird die Umstellung mit den 25. Mai 2018 nicht abgeschlossen sein, es sollten aber die wichtigsten Maßnahmen eingeleitet und weitere geplant sein.

WERBEBEITRAG | PRODUKTPORTRÄT

Integrität und Vertraulichkeit sichern

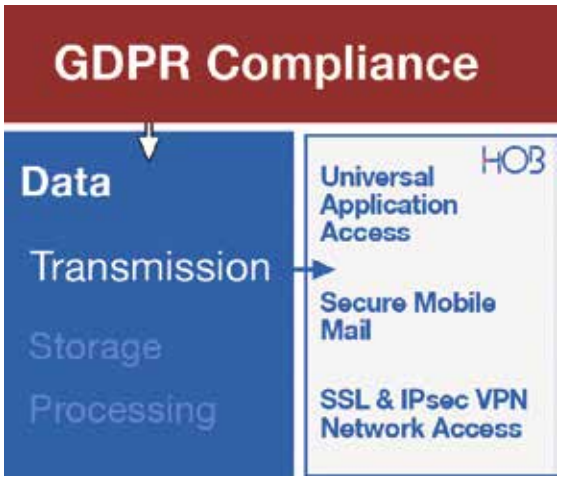
Hohe Geldbußen und sogar Gefängnisstrafen – die EU-DSGVO birgt viele Risiken, die Verunsicherung ist groß. Mit den sicheren Software-Produkten von HOB gehören die Sorgen darüber aber der Vergangenheit an.

Laut EU-DSGVO müssen alle personenbezogenen Daten verschlüsselt übertragen werden, zudem dürfen sie nicht zusammen mit dem Schlüssel übermittelt werden. HOB Lösungen schützen Ihre sensiblen Daten. Mit dem hochsicheren HOB-SSL (TLS) wird die Übertragung mit neuester Krypto-Technik verschlüsselt. Mitarbeiter können so schnell, bequem und auch sicher mit dem Unternehmen, der Cloud oder dem Internet verbunden werden.

Eine universelle und sichere, vom Bundesministerium für Sicherheit in der Informationstechnik (BSI) zertifizierte Connectivity-Plattform erhalten Sie mit HOB RD VPN – der anwenderfreundlichen Lösung, für die lokal nichts installiert werden muss. Mit HOBLink VPN Gateway können Sie Außenstellen, Anwendungen in der Cloud und einzelne Geräte Ihrer Mitarbeiter sicher anbinden. Dabei ist es mit allen IPsec-Clients und Gateways kompatibel.

Dank HOBLink Mobile können E-mails auch auf Smartphones absolut sicher und verschlüsselt abgerufen werden. Dabei werden keinerlei Daten auf dem Endgerät gespeichert. Bei einem Diebstahl des Geräts beschränkt sich der Schaden also ausschließlich auf den Materialwert – ein illegitimer Zugriff auf Firmendaten kann keinesfalls erfolgen.

www.hob.de/gdpr



Datenschutz nach EU-DSGVO - mit HOB kein Problem

ZU GUTER LETZT, ABER NICHT DAS LETZTE. EIN KOMMENTAR.

Cookies law

Sie gehört zum Stammtisch-Repertoire wie das Konferenzgebäck zum guten Meeting: Die nach der EU-Verordnung 1677/88 normativ gekrümmte Gurke. Nun soll nach Ansicht von Medienexperten der Keks um sein hart erkämpftes Plätzchen im digitalen Menü kämpfen müssen. Genauer gesagt geht es um den Cookie, das Grundnahrungsmittel der digitalen Wirtschaft. Oder auch der häufig nervigen Begleiterscheinung beim Surfen im Internet. Mit dem Inkrafttreten der EU-DSGVO will die EU nun ihre Bürger vor dem permanenten Auslesen, Speichern und Weiterverwenden ihrer Nutzungsdaten schützen (ePrivacy). Gleichwohl sind Cookies der fruchtbare Humus für Marketer, die ihre Früchte reifen und sie via Pay-per-Click das Haben-Konto wachsen lassen. „Opt-in" und „Kopplungsverbot" sollen künftig dafür sorgen, dass Anwender explizit ihr Einverständnis dazu geben müssen. Kein Click, kein Pay, kein Keks im Warenkorb. Cookies law? Facebook, Google, Amazon & Co schauen derweil genüsslich zu.

Karl-Heinz Möller
Chefredakteur

Unsere nächste Ausgabe

Handel der Zukunft

Der Handel ist im Wandel und hat im Bereich Digitalisierung eine neue Entwicklungsstufe erreicht. Doch noch nicht alle Unternehmen haben die digitalen Fähigkeiten schon für sich entdeckt. Konkrete Lösungskonzepte zeigen, wie die mit der Digitalisierung einhergehenden Herausforderungen gemeistert und die Chancen des Aufbruchs bestmöglich genutzt werden können.

Mehr am 27. Februar unter anderem im Handelsblatt. Und für alle, die nicht warten möchten, ab dem 26. Februar in unserer „Reflex Verlag" App. Zum Download einfach den QR-Code scannen.

IMPRESSUM

Projektmanager
Moritz Duelli
moritz.duelli@reflex-media.net

Redaktion
Karl-Heinz Möller,
Sven Dorseter,
Paul Trebol

Layout
Juan-F. Gallwitz
layout@reflex-media.net

Fotos
Thinkstock / Getty Images

Druck
BVZ Berliner Zeitungsdruck GmbH

V.i.S.d.P.
Redaktionelle Inhalte:
Karl-Heinz Möller
redaktion@reflex-media.net

Weitere Informationen:
Carolin Frank
carolin.frank@reflex-media.net

Reflex Verlag GmbH
Hackescher Markt 2–3
D-10178 Berlin
T 030 / 200 89 49-0

www.reflex-media.net

Eine Publikation der Reflex Verlag GmbH am 20. Februar 2018 im Handelsblatt.

Der Reflex Verlag und die Verlagsgruppe Handelsblatt sind rechtlich getrennte und redaktionell unabhängige Unternehmen.

WIR SIND DABEI

The Cyber Security People

Ultimative DSGVO-Checkliste für Zuspätkommer

www.it-sec.de/5vor12

it.sec
security for your information

Wir sprechen fließend DSGVO und ITSiG

- **Schutz Kritischer Infrastrukturen**
- **Datenschutz, Informationssicherheit & IT-Compliance**
- **Sicherheitsuntersuchungen & Penetrationstests**
- **Cybercrime – Prävention, Reaktion und Aufarbeitung**
- **National und international**

it.sec GmbH & Co. KG

Seit 1996 unterstützen unsere Informatiker und Juristen Unternehmen sowie staatliche und nicht staatliche Institutionen in mehr als 30 Ländern in Fragen zu Informationssicherheit, Datenschutz & IT-Compliance. Wir adressieren multi-regulatorische Anforderungen auch im internationalen Kontext, hacken uns im Auftrag in Online-Systeme und -Shops, Firmen, Banken oder industrielle Anlagen, helfen bei der Aufklärung von IT-bezogenen Sicherheitsvorfällen („Cybercrime") und bieten High-End Services für eDiscovery und eSearch Anforderungen.

Wir verfügen u. A. über die „Zusätzliche Prüfverfahrens-Kompetenz für §8a (3) BSIG" für Kritische Infrastrukturen.

it.sec GmbH & Co. KG
Einsteinstrasse 55
89077 Ulm (Germany)
Tel. +49 731 205 89 0
Fax +49 731 205 89 29
info@it-sec.de
www.it-sec.de

Hauptstadtbüro
Reinhardstr. 47
10117 Berlin-Mitte