Jetzt muss alles hinter Schloss und Riegel

Wer seine Datenverarbeitung nicht im Griff hat, kann ab Mai 2018 große Probleme bekommen. Warum die DATENSCHUTZ-GRUNDVERORDNUNG alle etwas angeht, welche Erfahrungen Unternehmer bereits damit machen und wer bei der Umsetzung hilft.

VON **BARBARA STEININGER**

Vor einem halben Jahr hatte Dieter Bernold „seinen Moment", wie er das nennt. In der Zeitung hatte der Personalentwickler von einer neuen Verordnung gelesen. Nichts ahnend schickte er eine Mitarbeiterin zu einer Informationsveranstaltung der Wirtschaftskammer, und die kam „ziemlich blass" zurück, wie er sich erinnert. Als die ihm zu erzählen begann, was es mit der sogenannten EU-Datenschutz-Grundverordnung (kurz DSGVO) auf sich hat, wurde ihm „erst einmal schummrig". Ende Oktober hat er seine Fassung wieder gefunden und ist für das, was da kommen wird, schon recht gut gerüstet (siehe Kasten Seite 24).

Dieser Realitätscheck steht den meisten Unternehmern erst bevor. Valide Zahlen zu dem Phänomen gibt es nicht, aber der enorme Zulauf zu einschlägigen Veranstaltungen schlägt alle Rekorde und weist durchaus Parallelen zur Einführung der Registrierkasse auf.

Datenschutzspezialist und Anwalt Rainer Knyrim ist seit Monaten auf

Hohe Strafen drohen: Schlendrian geht ins Geld

Maximale Strafen	Strafe alt	Strafe neu
Missachtung eines Datenschutzbescheids	25.000 Euro	**Bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes**
Verletzung des Auskunftsrechts	500 Euro	
Verletzung des Löschungsrechts	500 Euro	
Unrechtmäßige Datenspeicherung	nicht strafbar	
Unzulässige Auslandsübermittlung	10.000 Euro	

VERWALTUNGSSTRAFE. Firmen drohen hohe Strafen. Ob Geldbußen über Behörden verhängt werden, bleibt den Staaten überlassen: Hier wechselt „ja nur" Steuergeld den Besitzer. In Österreich werden gegen Behörden keine Strafen verhängt.

Was sind personenbezogene Daten eigentlich?

Alle Daten, die eine Person identifizieren können: Name, Geburtsdatum, Geburtsort, Arbeitgeber, Telefonnummer, E-Mail-Adressen, Passnummer, Kreditkarten- und Bankdaten, Sozialversicherungsnummer, Cookies, IP-Adressen, Standortdaten etc.

Vortragstour in den Bundesländern, hat vor einigen Tausend Unternehmern gesprochen und erwartet auch zur „Datenschutz-Grundverordnung-Convention“ am 30. 10. bis zu 1.000 Zuhörer in der Messe Wien. „Es ist *das* Rechtsthema 2017 und wohl auch für 2018“, sagt er, „und es sind nicht nur Kleinfirmen, die sich erst jetzt erstmals damit beschäftigten. Ich weiß von 5.000-Mitarbeiter-Konzernen, die das noch vor sich haben.“

Warum das Thema Datenschutz ausgerechnet jetzt im Wortsinne elektrisiert, ist simpel: Wer die neuen Regeln nicht einhält, dem drohen Strafen von bis zu 20 Millionen Euro oder vier Prozent des weltweit (nicht nur lokal) erzielten Jahresumsatzes. Fehler können hier richtig teuer werden. Die maximale Strafhöhe hat unlängst der bekannte Datenschutzaktivist und Jurist Max Schrems als „zu hoch“ eingestuft: „Große Konzerne haben vier Prozent des Umsatzes zu befürchten, was gut ist. Leider sind Strafen von bis zu 20 Millionen Euro für KMU zu viel. Für Einpersonenunternehmen hätten vielleicht auch 100.000 Euro gereicht.“

WAS STECKT HINTER DER VERORDNUNG? Die DSGVO trat bereits am 24. Mai 2016 in Kraft, gilt ab dem 25. Mai 2018 in allen EU-Mitgliedsstaaten und muss von den Einzelstaaten individuell umgesetzt werden. In Österreich wurde dafür das Datenschutzgesetz Ende Juni im Eiltempo novelliert – unter heftigen Protesten von Kritikern, die der Regierung „Datenschutz-Pfusch“ vorwerfen, weil keine der 109 Stellungnahmen berücksichtigt wurde.

WAS BEDEUTET DIE VERORDNUNG? Für Unternehmen ist das Wichtigste, dass sie einen „Paradigmenwechsel nachvollziehen müssen“, wie Felix Hörlsberger von der Kanzlei Dorda Brugger Jordis das nennt: „Ich frage nicht die Behörde, was muss ich tun, sondern ich muss die notwendigen Maßnahmen von mir aus setzen. Erst wenn etwas schiefgeht, tritt die Behörde auf den Plan. Der Grundgedanke dahinter ist, dass jeder, der Daten verarbeitet, sich selbst darum kümmern muss, dass er sie schützt.“

Mit der Verordnung kommen auch ein paar neue Begriffe auf Unternehmen zu, etwa die Datensparsamkeit (es dürfen nicht überschießend ohne Zweck Daten gesammelt werden), die Speicherbegrenzung (Daten müssen gelöscht werden, wenn sie nicht mehr benötigt werden) oder die Pseudonymisierung (Daten sollten „codiert“, also nicht mit Klarnamen in Datenbanken gespeichert sein).

WER IST DAVON BETROFFEN? Alle Unternehmen, die in irgendeiner Art und Weise personenbezogene Daten verarbeiten (Definition oben). Die Firmengröße spielt keine Rolle, auch EPU und Kleinfirmen sind betroffen, wie auch Vereine und Behörden. Wer in der EU Waren oder Dienstleistungen anbietet, ist auch dann betroffen, wenn er hier keinen Firmensitz hat: Konzerne außerhalb der EU können sich dieser Verordnung also nicht entziehen und müssen einen lokalen Vertreter bzw. Ansprechpartner nominieren. Wer einen Datenvorfall, etwa einen Hackerangriff, erlitten hat, muss ihn binnen 72 Stunden der Datenschutzbehörde melden. ►

FALLSTUDIE KONZERN

A1 begann schon sehr früh mit der Arbeit an der DSGVO und überprüft unter anderem sämtliche Kunden- und Lieferantenverträge.

Fast schon vorbildlich früh wurde das Thema gestartet: „Erste Drafts haben wir 2015 entwickelt und Anfang 2016 ein Kick-off mit den Vorständen gemacht“, sagt Judith Leschanz, die zuständige Managerin. Für die Umsetzung gibt es ein bereichsübergreifendes Programm und einen zentralen Datenschutzbeauftragten als Schnittstelle zur Behörde. Pro Fachbereich gibt es eine Person, die Datenschutzaspekte verantwortet. Stark betroffen sind Marketing- und Technikabteilungen, so müssen alle Kunden- und Lieferantenverträge angepasst werden.

Das erste konkrete Projekt war die „Einwilligungserklärung neu“, wo sämtliche Kundenverträge überprüft und gegebenenfalls ergänzt werden, um die notwendige Transparenz und die eindeutige Zustimmung zur Verarbeitung der Daten sicherzustellen. „Dafür haben wir ein Selfcare-Tool entwickelt. Die neuen Einwilligungserklärungen werden in einer zentralen Datenbank hinterlegt und sind bindend für die weitere Verarbeitung.“ Die Mitarbeiter sind sensibilisiert: Im November beginnen weitere Schulungen via E-Learning. Betroffen ist nicht nur die Österreich-Tochter, sondern alle A1-Länder. Leschanz: „Von der Idee, ein gemeinsames großes Projekt zu machen, sind wir abgekommen. Das hätte uns verlangsamt. Wir bauen auf Vernetzung, lokale Optimierung und helfen uns gegenseitig mit Best Practices bei der Umsetzung.“

JUDITH LESCHANZ, A1. „Siebenstellig wird es schon werden“, schätzt die Managerin die Kosten für die DSGVO-Umsetzung bei A1 in Österreich.

FOTOS: ISTOCKPHOTO, FOTO WEINWURM GMBH

FALLSTUDIE KLEINFIRMA

Der Personalentwickler Argo ist schon bereit für den Mai 2018 und weiß auch schon ziemlich genau, was ihn die DSGVO kostet.

Seit einem halben Jahr arbeitet das 20-Mitarbeiter-Unternehmen Argo an der Umsetzung der DSGVO. Der Personalentwickler hat zwar keine riesigen Kundendatenbanken, aber mit 360-Grad-Feedbackanalysen und Persönlichkeitsprofilen doch mit „sehr sensiblem Datenmaterial zu tun", sagt Geschäftsführer Dieter Bernold, der unter anderem drei praktische Auswirkungen auf seinen Geschäftsalltag beschreibt: „Personalakten werden wir nicht mehr per E-Mail versenden, sondern wir geben nur mehr gesicherte Zugänge in eine Cloud an, doppelt abgesichert mit PIN-Code. Teilnehmerlisten von Seminaren haben wir früher aufbewahrt, das machen wir nicht mehr. Lohnabrechnung via PDF an den Steuerberater schicken zu können, ist Geschichte." Eine ganz profane Änderung tut ihm besonders leid: „Bei Seminargruppen wurden natürlich auch Fotos gemacht. Diese emotionalen Erinnerungen werden nur möglich sein, wenn es das schriftliche Einverständnis aller gibt, ein unverhältnismäßig hoher administrativer Aufwand." Sensibilisierung für das Thema findet er sinnvoll, hält die Strafen aber für überzogen und hofft, dass die neue Auskunftspflicht nicht allzu viel administrative Arbeit für Unternehmen verursacht und damit wertvolle Ressourcen für die eigenen Kunden blockiert.

DIETER BERNOLD, ARGO, ÜBER DIE KOSTEN: „20.000 bis 35.000 Euro. Zusätzlich gehen bis zu 60 interne Personentage Arbeit in das Projekt."

► **WELCHE RECHTE HAT DIE PERSON, DEREN DATEN GESPEICHERT WERDEN?** Schon bisher konnten Kunden eine Datenauskunft bei Unternehmen beantragen und die Löschung bzw. Berichtigung verlangen. Mit der neuen Verordnung kommt das Recht dazu, diese Verarbeitung einzuschränken – das muss allerdings begründet werden. Die Unternehmen müssen all das innerhalb einer Frist von einem Monat erfüllen. Diese kann in besonders komplexen Fällen oder bei besonders vielen Anfragen auf drei Monate verlängert werden – was vom Unternehmen aber sehr gut begründet werden muss.

Ebenfalls neu ist das Recht auf Datenübertragbarkeit. Betroffene sollen ihre personenbezogenen Daten von einem Unternehmen zum nächsten „mitnehmen" können, ohne dass es technische Barrieren gibt und dafür Gebühren verlangt werden. In der Praxis rechnen Experten allerdings mit größeren Schwierigkeiten in der Umsetzung. Beispiel: Als foodora-Kunde kann ich verlangen, dass meine Daten an UberEats weitergereicht werden.

WER BRAUCHT EINEN DATENSCHUTZBEAUFTRAGTEN? Zwingend ist der nur für Behörden und öffentliche Stellen sowie Unternehmen, deren Kerntätigkeit regelmäßige umfangreiche Überwachung ist (etwa Detektive) oder die als Kerntätigkeit besondere Datenkategorien wie etwa Gesundheitsdaten verarbeiten (z. B. Krankenhäuser). Der Datenschutzbeauftragte kann ein eigener Mitarbeiter sein, man kann aber auch einen externen Datenschutzbeauftragten nominieren, etwa einen Anwalt oder einen dafür zertifizierten Anbieter.

WER KONTROLLIERT, WER STRAFT? Üblicherweise wendet sich eine Person mit einem Anliegen wie Auskunft oder Löschung an das Unternehmen und bekommt die Auskunft oder die gewünschte Aktion durchgeführt. Gibt es hier Probleme, kann sich die Person an die nationale Datenschutzbehörde wenden, die ein Verfahren einleitet und Geldbußen von bis zu 20 Millionen Euro oder vier Prozent vom Umsatz verhängen kann. Ein erlittener Schaden muss aber nachgewiesen werden bzw. dann vor Gericht eingeklagt werden. Der Schadenersatz muss vor Gericht verhandelt werden.

WAS BEDEUTET DAS FÜR EXTERNE DIENSTLEISTER? Unternehmer müssen sicherstellen, dass auch ihre externen Dienstleister nach der neuen Verordnung arbeiten. „Sie müssen die Verträge mit ihren Auftragsverarbeitern diesbezüglich überprüfen, sofern solche überhaupt schon bestehen", sagt Anwalt Rainer Knyrim.

Wer Daten in eine Cloud gibt und dadurch Daten in ein Drittland übermittelt, muss sich ebenfalls vertraglich absichern, dass die Datenverarbeitung sicher ist. Sollte es etwa im Zuge eines Hackerangriffs zu einer Datenschutzverletzung beim Dienstleister kommen, haftet unter Umständen der Unternehmer, der die Cloud-Dienste in Anspruch nimmt, wenn er einen gewählt hat, der nicht über ausreichende Sicherheitsmaßnahmen verfügt.

„Es ist *das* Rechtsthema 2017 und wohl auch für 2018. Nicht nur Kleinfirmen beschäftigen sich erst jetzt damit, auch 5.000-Mitarbeiter-Konzerne haben das noch vor sich."

RAINER KNYRIM
ANWALT, DATENSCHUTZEXPERTE

WAS MÜSSEN KLEINSTUNTERNEHMEN BEACHTEN? Natürlich gilt die DSGVO auch für sie. EPU müssen sich fragen, welche Daten sie von ihren Kunden haben, ob diese sicher gespeichert sind, und sie müssen bereit sein, ihrer Auskunftspflicht nachzukommen. Vorhandene Datenbanken werden damit aber nicht automatisch Makulatur. Man sollte sich aber informieren, ob für künftige Mailings oder Marketingaktionen Anpassungsbedarf besteht.

WIE STELLE ICH FEST, OB ICH BEREIT FÜR DIE VERORDNUNG BIN? Am Beginn sollte eine Bestandsaufnahme stehen, in die führende Mitarbeiter aus den Schlüsselabteilungen eingebunden sind: Die Projektverantwortlichen sollten in den Fachabteilungen, vor allem aber in der Personal-, der IT- und der Marketingabteilung erheben, welche Daten im Unternehmen sind, wie sie verarbeitet werden und mit welchen externen Dienstleistern man zusammenarbeitet. Für absolute Neulinge im Thema könnte ein Selbstcheck (siehe rechts) am Beginn stehen oder auch einschlägige Seminare. Das Zuratenziehen von Experten in Form von externen Beratern ist zu empfehlen.

WIE SETZT MAN SO EIN PROJEKT PRAKTISCH UM? Wie schon in der Bestandsaufnahme müssen auch in der konkreten Umsetzung alle Abteilungen miteinbezogen werden und alle Mitarbeiter für das Thema sensibilisiert bzw. geschult werden. In Konzernen wie einer A1 sind Tausende Mitarbeiter davon betroffen (siehe Fallbeispiel Seite 23). Managementberater Lambert Gneisz sagt: „Die Datenschutz-Grundverordnung ist ein neuer Teil des betrieblichen Risikomanagements und das Risiko hat sich massiv verändert."

Nach der Bestandsaufnahme sollten Arbeitsgruppen gebildet und Zeitpläne erarbeitet werden. Es gibt einigen administrativen Aufwand, vor allem zu Beginn: Unternehmen müssen ein Verzeichnis für Verarbeitungstätigkeiten anlegen – das meint das konkrete Niederschreiben der Datenerfassung und -verarbeitung im Unternehmen.

ONLINE-SELBSTCHECK. Es gibt viele Ersttests für das Thema. Die Wirtschaftskanzlei PHH hat 150 Fragen entwickelt, die HR, IT, Geschäftsführung und Marketing separat beantworten und die dann zusammengeführt werden. 3.000 Euro kostet diese Bestandsaufnahme, die bei einem Auftrag natürlich gegengerechnet wird. *datenschutz-phh.at*

Viel Zeit ist nicht mehr bis zum kommenden Mai: Aber für die vielen Unternehmer, die sich noch gar nicht mit dem Thema beschäftigt haben, ist in den rund 150 Werktagen einiges zu schaffen. Obwohl da und dort hektischer Aktionismus ausgebrochen ist, sind Panikreaktionen unangebracht, sind sich Experten einig. Welche Beschwerden es von den betroffenen Personen geben wird und in welcher Höhe Strafen in Österreich dann tatsächlich ausgesprochen werden, wird sich in der zweiten Jahreshälfte zeigen.

Natürlich empfinden viele Unternehmer die DSGVO als Schikane, der organisatorische und finanzielle Aufwand ist erheblich. Und doch gibt es vor allem unter jenen, die ihre Hausaufgaben bereits gemacht haben, auch positive Bilanzen. Manche haben ihre Kundendaten endlich wieder einmal auf dem aktuellen Stand, andere sind im Zuge dieses Change-Projekts sogar auf neue Ideen gekommen. Personalentwickler Bernold ist über die Kosten nicht happy, sieht die Sache mittlerweile aber auch pragmatisch: „Wir sind dadurch noch ordentlicher im Arbeiten geworden, und ich hoffe doch, dass wir den Umstand, dass wir schon DSGVO-konform sind, auch im Marketing einsetzen können." T

SERVICE

WER IHNEN BEI DER DSGVO HELFEN KANN

Ausgewählte Events und Initiativen.

Ein Riesenthema ist die DSGVO bei der Wirtschaftskammer, die viele Information und Veranstaltungen anbietet. Am 30. Oktober veranstalten die Kammern Wien und NÖ einen Datenschutzkonvent in der Messe Wien. Für KMU und EPU gibt es zehn Workshops bis Jahresende (fast ausgebucht). Gefördert werden auch externe Beratungsleistungen. Es sind Referenten allein für dieses Thema abgestellt, um Mitgliedern Auskunft zu geben, etwa im Handel. *wko.at/datenschutz*

→ **Die Post hat zum Thema ein eigenes Trainingsformat aufgesetzt und informiert in Halb- oder Ganztagesschulungen sowohl Neulinge als auch Fortgeschrittene sowie Juristen. Für November gibt es noch Termine.** *post.at/data-academy*

→ **A1, Bundesrechenzentrum, ORF, Drei, Casinos Austria u. a. haben einen Verein gegründet, wo sie sich gegenseitig bei dem Thema helfen. Über die Website *privacyofficers.at* können Interessierte beitreten, und es gibt laufend neue Informationen.**

→ **Eine gute Adresse für Informationen zum Thema ist die ARGE Daten, die unterschiedliche Fachseminare anbietet und auch Datenschutzbeauftragte ausbildet.** *argedaten.at*

→ **Nicht zuletzt informieren viele Anwälte über die DSGVO, bieten ihren Kunden zahlreiche hausinterne Informationsveranstaltungen an und beraten, welche juristischen Konsequenzen die DSGVO für das eigene Geschäftsmodell hat.**

FOTOS: BEIGESTELLT (2), STEPHAN HUGER