DATEN WERDEN ZUM RISIKO

Der Countdown läuft: Warum Unternehmer die Datenschutzgrundverordnung kennen sollten und Unwissenheit nicht vor STRAFE schützt.

VON **BARBARA STEININGER**

Eingetragen haben sich den 25. Mai 2018 noch nicht alle Unternehmer: Das sollten sie aber, denn ab dem Stichtag gehen sie ihren Geschäften mit erhöhtem Risiko nach. Mit jenem Freitag gilt die sogenannte Datenschutzgrundverordnung (DSGVO) in allen EU-Mitgliedsstaaten. Und anders, als es viele Betroffene vom Projekt Registrierkasse in Erinnerung haben, wird es bei dieser Verordnung keine Nach- und Umstellungsfristen geben, denn in Kraft getreten ist die DSGVO eigentlich bereits vor zwei Jahren.

Mit der DSGVO wurde der Umgang mit personenbezogenen Daten neu geregelt, und das betrifft ausnahmslos alle Unternehmen und Organisationen, die solche Daten haben und verarbeiten: gleichgültig, ob es sich um ein Kleinstunternehmen handelt, eine Schule oder den lokalen Sozialdienst. Gemessen an der Bedeutung dieser Verordnung – die ARGE Daten stuft sie glatt als „größte Revolution in der Informationsverarbeitung seit der Erfindung des PC“ ein –, stehen ihr viele Betroffenen oft ratlos gegenüber, so sie sich damit überhaupt schon beschäftigt haben.

Experten, die sich mit dem Thema auseinandersetzen, berichten in Übereinstimmung von Phänomenen, die von ►

FOTO: ISTOCKPHOTO

► Panik bis zu Ignoranz reichen. Axel Anderl von der Kanzlei Dorda Brugger Jordis bringt seine Eindrücke auf den Punkt: „Manche glauben noch immer, dass das ein Nischenthema ist, das sie nicht betrifft. Viele wollen nicht glauben, dass es tatsächlich Strafen geben wird."

Wie viele sich auf die DSGVO bereits vorbereitet haben, kann nur geschätzt werden. „Selbst bei optimistischen Schätzungen auf Basis unserer Brancheneinsicht muss davon ausgegangen werden, dass noch immer mehr als die Hälfte der Betroffenen keinerlei oder unzureichende Vorkehrungen getroffen hat."

Dieser Realitätscheck steht vielen also bevor, und etliche bekommen veritable Wut- oder Beinahe-Ohnmachtsanfälle wie jüngst bei einem Vortrag in der Versicherungsbranche. Valide Zahlen zu dem Phänomen gibt es nicht, aber der enorme Zulauf zu einschlägigen Veranstaltungen schlägt alle Rekorde.

WAS ÄNDERT SICH? Verknappt gesagt, müssen sich Unternehmer und Organisationen, die personenbezogene Daten haben, sicherstellen, dass sie mit diesen Daten sorgsam und verhältnismäßig umgehen. „Wie fahrlässig Unternehmen mit heiklen Daten umgehen, offenbaren nicht nur spektakuläre Datendiebstähle", sagt Markus Knasmüller von BMD: „Bislang bezahlten Unternehmen so etwas nur mit einem Imageverlust, und viele haben das leider mit einkalkuliert."

Der Datenschutz an sich ist nicht neu, wird mit der DSGVO allerdings neu geregelt. Elementarste Neuerung: Das Risiko verlagert sich hin zum Unternehmen. Anwalt Anderl: „Früher musste man der Behörde die Verarbeitung von Daten melden. Das entfällt nun. Die Unternehmen müssen selbst Verzeichnisse aller Datenverarbeitungen führen und dürfen entscheiden, ob und wie sie Daten verarbeiten dürfen. Sie tragen aber auch das volle Risiko dafür."

Warum das Thema Datenschutz ausgerechnet jetzt elektrisiert, ist rasch erklärt: 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 und Fahrlässigkeit können teuer werden.

Wie diese EU-Verordnung in Österreich umgesetzt wird, regelt das nationale Datenschutzgesetz, das im Juni 2017 novelliert wurde und einiges an Kritik provozierte („Datenschutz-Pfusch"). Im dem Gesetz sind einige Öffnungsklauseln berücksichtigt, die den Spielraum in bestimmten Fällen erweitern: Die Datenverarbeitung für statistische Zwecke, Forschungsfälle oder der Katastrophenfall sind hier geregelt, aber auch das Alter für Kinder festgelegt, ab wann sie digitalen Diensten selbst zustimmen können.

Ultimative Rechtssicherheit ist mit Ende Jänner 2018 aber noch nicht gegeben. „Im Regierungsprogramm wird auf Seite 81 die Weiterentwicklung des österreichischen Datenschutzregimes angekündigt", sagt Anwalt Rainer Knyrim, „es kann also sein, dass es noch vor Inkrafttreten des Gesetzes eine Novelle gibt. Es bleibt spannend."

Mit einer gewissen Rechtsunsicherheit werden Betroffene bis auf weiteres leben müssen, denn zu 100 Prozent kann ein Strafrisiko auch dann nicht ausgeschlossen werden, wenn die DSGVO-Basisvereinbarungen eingehalten sind.

HOHE BUSSGELDER: Schlechter Datenschutz kostet

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 auch über Behörden verhängt werden, bleibt den EU-Mitgliedsstaaten überlassen: Hier würde ja „nur" Steuergeld den Besitzer wechseln. In Österreich werden gegen Behörden keine Strafen verhängt.

Wie gut sind Unternehmer auf die DSGVO vorbereitet?

28 % sind komplett ahnunglos, was die DSGVO betrifft.

26 % wissen Bescheid, können die Frist aber nicht halten.

51 % glauben, dass die DSGVO für KMU zu kompliziert ist.

52 % sehen ein, dass Datenschutz besser werden muss.

FOTO: LUKAS ILGNER

Bei einem Newsletter den Verteiler für alle Empfänger sichtbar mitzuschicken, kann teuer werden. Ebenso das Sammeln von Kundendaten auf Zetteln im Geschäft, wo sich andere bereits eingetragen haben.

WER IST DAVON BETROFFEN? Ausnahmslos alle Unternehmen, die in irgendeiner Art und Weise personenbezogene Daten verarbeiten. Die Größe spielt keine Rolle, auch Kleinstfirmen sind betroffen, ebenso 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.

Dieser muss dann den Rechten der Betroffenen – nach Auskunft, Löschung und Berichtigung von Daten – entsprechen. Das war früher schon möglich, mit der DSGVO kommt das Recht dazu, diese Verarbeitung einzuschränken, das muss aber begründet werden.

Die Unternehmen müssen all das innerhalb einer Frist von einem Monat gewährleisten, und das kann eng werden für jene, die nicht gut organisiert sind. In besonders komplexen Fällen oder bei besonders vielen Anfragen kann die Frist auf drei Monate verlängert werden – muss aber wiederum vom Unternehmen gut begründet sein.

Neu ist das Recht auf Datenübertragbarkeit. Betroffene sollen ihre 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. Die Idee dahinter ist, den Verbrauchern einen einfacheren Dienstleisterwechsel zu ermöglichen. Von Bank A zu Bank B wechseln, von Netzwerk A zu Netzwerk B. Experte Knasmüller: „Der Datenhalter muss nur jene Daten für den Wechsel freigeben, die er initial vom Kunden erhalten hat. Seine daraus abgeleiteten Erkenntnisse aber nicht. In der praktischen Umsetzung wird das aber noch interessant werden." Unternehmer müssen zudem sicherstellen, dass ihre externen Dienstleister nach der neuen Verordnung arbeiten. „Sie müssen die Verträge mit ihren Auftragsverarbeitern überprüfen, sofern solche überhaupt schon bestehen", rät Anwalt Knyrim. Wer Daten in eine Cloud gibt und dadurch Daten in ein Drittland übermittelt, muss sich vertraglich absichern, dass die Datenverarbeitung dort sicher ist. Denn sollte es im Zuge eines Hackerangriffs zu einer Datenschutzverletzung bei einem externen Dienstleister ohne ausreichende Sicherheitsmaßnahmen kommen, haftet unter Umständen der Unternehmer, der die Dienste in Anspruch nimmt.

Auch Datendiebstähle unter den Teppich zu kehren, ist künftig nicht mehr möglich: Der geübte „Totstellreflex" wird künftig streng bestraft. Es gilt eine 72-Stunden-Meldepflicht für Vorfälle.

WER KONTROLLIERT DAS ALLES? WER STRAFT? Personen, die Auskunft oder Löschung von Daten begehren, wenden sich im ersten Schritt direkt an das Unternehmen oder die Organisation. Sollte er hier zu Problemen kommen, ist die nationale Datenschutzbehörde die nächste Anlaufstelle. Die neue Regierung hat sie nun dem Justizministerium (bislang Bundeskanzleramt) unterstellt, und die Leiterin Andrea Jelinek hat schon einmal „mehr Personal beantragt für die mannigfachen Tätigkeiten, die neu auf ►

Ein besonders sensibler Bereich sind die Schulen: Direktoren und Pädagogen sollten sich Gedanken machen, was mit den Schülerdaten passiert: Das beginnt beim Klassenfoto, Noten und reicht bis zum Gesundheitszustand. Werbung an der Schule wird definitiv heikler.

SERVICE

WICHTIGE PUNKTE UND FACHBEGRIFFE

Ausgewählte Fachbegriffe, kurz erklärt.

→ **Personenbezogene Daten: Darunter werden alle Daten verstanden, mit denen eine Person identifiziert werden kann: Name, Geburtsdatum und -ort, Arbeitgeber, Telefonummer, E-Mail-Adressen, Passnummer, Kreditkarten- und Bankdaten, SV-Nummer, IP-Adressen, aber auch Cookies und Standortdaten. Sensible Daten – sexuelle, religiöse oder politische Orientierung, Gesundheitsdaten etc. – müssen noch besser geschützt werden.**

→ **Wichtige neue Termini der DSGVO sind u. a. Datensparsamkeit (Daten dürfen nicht überschießend, ohne Grund gesammelt werden) und Speicherbegrenzung (Daten müssen gelöscht werden, wenn sie für den initialen Zweck nicht mehr benötigt werden, außer es gibt gesetzliche Verpflichtungen dazu, wie bei Finanzdaten). Ganz wichtig: Wird der Datenschutz verletzt (etwa durch einen Hackerangriff oder Datendiebstahl), muss das der Behörde binnen 72 Stunden gemeldet werden.**

→ **Das Recht auf Auskunft gab es bereits, ebenso die Möglichkeit, Daten berichtigen zu lassen, unter der DSGVO wurden Details aber neu geregelt: Unternehmen müssen binnen eines Monats Auskunft geben, u. a. mit einem vollständigen Ausdruck der Daten. Im begründeten Fall kann diese Frist auf drei Monate ausgedehnt werden. Werden umfangreiche Konvolute abgefragt, darf das Unternehmen verlangen, dass das Auskunftsersuchen präzisiert wird.**

→ **Neu geschaffen wird der Job eines Datenschutzbeauftragten: Zwingend ist der nur für Behörden und bestimmte Firmen mit besonders sensiblen Daten (Detektive, Krankenhäuser etc.). Den Job kann ein eigener Mitarbeiter oder ein externer Dienstleister übernehmen, den man nominiert: einen Anwalt oder dafür zertifizierten Anbieter.**

► uns zukommen“. Diese Behörde wird künftig auch mehr an öffentlicher Aufmerksamkeit zuteil werden als bisher, und das vor allem deshalb, weil sie bei Verstößen gegen die DSGVO die Verfahren einleitet und Geldbußen aussprechen wird. Jelinek zur geplanten Vorgangsweise: „Unser Fokus liegt darauf, allfällige Verfahren zu führen und auch die Compliance der Unternehmen zu überprüfen. Wir werden (auch) Verwaltungsstrafverfahren führen, wenn erforderlich und geboten. Die DSGVO sieht aber auch die Möglichkeit der Warnung und Verwarnung vor.“

Zur Höhe von Bußen sagt sie: „Sollten Geldbußen zu verhängen sein, stellen wir sicher, dass sie wirksam, verhältnismäßig und abschreckend sind. Schon aus dieser Formulierung ergibt sich, dass die Verhältnismäßigkeit bei Verhängung von Geldstrafen gegeben sein muss.“ Die Geldstrafen fließen ins allgemeine Staatsbudget. Schadenersatz bekommen Betroffene nur, wenn sie einen solchen vor Gericht nachweisen können.

Wie sorgsam mit Daten umgegangen wird, wird nicht nur Juristen und IT-Dienstleister beschäftigen. Datenschutz und Privatsphäre werden auch in der Öffentlichkeit stärker diskutiert werden. Den 25. Mai haben sich auch bekannte Datenschützer wie der Jurist Max Schrems vorgemerkt. Er hat mit Mitstreitern eine Art „VKI für Datenschutz“ namens noyb (none of your business) gegründet und will Unternehmen und Organisationen, die das Thema noch immer nicht ernst nehmen, auf die Finger schauen – mit Klagen, aber auch mit Aufklärungsarbeit.

WAS KOSTET DAS GANZE? Was die Umsetzung der DSGVO kostet, hängt von der Unternehmensgröße, Mitarbeiteranzahl, Geschäftsmodell und Art der Daten ab, die verarbeitet werden. Für große Konzerne bewegen sich die Kosten gut und gern im Bereich von ein paar Hunderttausend Euro, eine halbe Million ist nicht zu hoch gegriffen. Da und dort geht es um Dimensionen, die nicht einfach zu stemmen sind. Anwalt Anderl weiß, dass die DSGVO gerade die Start-up-Szene in Aufruf versetzt: „Viele arbeiten im Healthcare- oder Sportbereich, da sind natürlich sensible Daten betroffen.“ Wer von einer 100.000-Euro-Finanzierungsrunde gleich einmal 40.000 Euro in ein Datenschutzprojekt stecken muss, wird nicht begeistert sein. Eine Strafe kann einem aber auch später das Genick brechen oder einen Exit erschweren – alles eine Frage der Risikoabwägung.

Die Betriebsärztin führt seit vielen Jahre ein informelles Impftagebuch, weiß also, wer wann die letzte Zeckenimpfung bekommen hat. Das war ein praktischer Service, müsste künftig aber vereinbart werden.

Einzelunternehmer hingegen, die gewillt sind, sich zumindest ins Thema einzulesen, brauchen mit der DSGVO keine hohen Kosten zu kalkulieren, abgesehen von der eigenen Arbeitszeit. „Musterverträge und Vorlagen für Verfahrensverzeichnisse können sich WKO-Mitglieder dort kostenlos herunterladen“, sagt Anwalt Knyrim. Er hört von vielen Seiten, dass die Softwareanbieter unter Druck kommen. Unternehmer wollen dem Recht auf Datenlöschung nachkommen, merken aber, dass ihre Datenbanken gar nicht dafür ausgelegt sind. Knyrim schildert einen typischen Gesprächsverlauf: „Der Kunde sagt, wir müssen löschen, also programmiert uns das. Der Anbieter sagt, wir können den Kunden ganz löschen oder gar nicht.“

Einen Kunden komplett aus der Datenbank zu löschen, wäre Harakiri. Knyrim rät: „Überlegen Sie sich genau, welchen Datenbestand sie in ihrer Datenbank haben und wie sie damit umgehen.“ Er bringt das Beispiel eines Klienten: Das Unternehmen schrieb 1.500 Kunden an mit der Bitte um Zustimmung zur Datenverarbeitung, andernfalls würden sie aus der Datenbank gelöscht. „Weniger als 100 haben zurückgeschrieben und die Zustimmung erteilt. So vernichten sie ihre Kundendatenbank mit unüberlegtem Aktionismus.“ Worum sich die größten Sorgen vieler Unternehmen drehen werden, ist der Umgang mit historischen und neuen Kundendaten. „Die Datenschutzbehörden haben angedeutet, dass man, wenn man die Zustimmung des Kunden nicht belegen kann, diesen Altbestand auch nicht verwenden darf“ zitiert Knyrim aus Arbeitspapieren der Datenbehörden, die sich als Artikel-29-Gruppe regelmäßig abstimmen.

Neben der IT- und Rechtsabteilung wird vor allem die Marketingabteilung durch die DSGVO viel zu tun bekommen, erläutert Anderl: „Wie ich die Zustimmung der Kunden erhalten habe, ist heikel. Die gängige Praxis, ich hole mir die Daten über ein Gewinnspiel oder ich hole die Zustimmungserklärung AGB ein, ist unter der DSGVO kritischer. Es darf kein Zwang bestehen, dass Leistungen nur bei Preisgabe dafür nicht benötigter Daten bezogen werden können. Als Unternehmer muss ich auch genau sagen, was ich mit den Daten mache.“

Je nach Geschäftsmodell wird es natürlich Abteilungen und Branchen geben, die stärker von der DSGVO betroffen sein werden: Ein Handwerksbetrieb wird weniger vorbereitende Vorkehrungen treffen müssen als ein Personaldienstleister.

Angesichts der Granularität und Qualität ihres Datenbestands stark betroffen ist die HR-Branche. Umso mehr erstaunen Umfragen wie die von SD Worx unter Personaldienstleistern: 44 Prozent haben keine Ahnung, worum es in der DSGVO überhaupt geht. Andere Branchen sind alarmiert, aber verunsichert ob der Auslegung im Einzelfall. Marion Rossmann von Rossmann Casting beschreibt die Problematik: „In einer Schauspielerakte stehen nicht nur personenbezogene Daten, sondern auch sensible Daten drin – von detaillierten biometrischen Merkmalen bis hin zu Essensgewohnheiten. Bevor ein Schauspieler aber überhaupt zum Casting eingeladen wird, werden Besetzungslisten erstellt und abgeglichen. Die DSGVO würde unsere bisherigen Arbeitsprozesse komplett über den Haufen werfen. Wie wir die DSGVO umsetzen können, diskutieren wir gerade auch mit deutschen Branchenkollegen.“

Wer seine Mitarbeiter mit Videoüberwachung oder mittels Standortdaten, etwa bei Lieferdiensten, überwacht, muss mit dem Betriebsrat Vereinbarungen schließen bzw. diese erneuern. Zweckmäßigkeit, Dauer und Inhalte sind unter der DSGVO neu zu justieren.

WAS GEHT SICH NOCH AUS? Viel Zeit bleibt also nicht mehr bis zum 25. Mai, und eine der meistgehörten Fragen, die Knyrim in seinen Seminaren gestellt wird, ist: worauf man sich angesichts der kurzen Zeitspanne konzentrieren soll. „Man sollte ein Verfahrensverzeichnis anlegen, also wissen, wo im Unternehmen welche Daten verarbeitet werden. Man soll die neuen Informationspflichten einhalten können. Und man sollte überprüfen, ob man Auskunfts- und Löschanfragen nachkommen kann.“

RAINER KNYRIM, DATENSCHUTZEXPERTE: „Vernichten Sie nicht Ihre Kundendatenbank mit unüberlegtem Aktionismus.“

Was wird am D-Day passieren, fragen sich viele: Das Recht auf Datenauskunft bestand ja auch schon bisher, wurde aber verhältnismäßig wenig wahrgenommen. Das wird sich ändern, sind sich alle Experten einig, die Frage ist, in welchem Ausmaß das passieren wird. Knasmüller berichtet von verunsicherten Unternehmern, die fürchten, dass ihr Tagesgeschäft unter der Last von vielen Datenschutzauskunftsbegehren leidet.

Anwalt Anderl hat das Datenschutzteam über die letzten Jahre personell massiv verstärkt. Dennoch besteht für ihn und sein Team bis zum Stichtag strikte Urlaubssperre. Er rechnet mit einer kurzen Verschnaufpause nach dem 25. Mai, da das Thema in Wellen weiter aktuell bleiben wird: Zuerst werden die Nachzügler ihre Projekte mit einer entsprechenden Priorität starten, und „sobald die erste Strafe einmal verhängt wird“, kommt der nächste Schwung.

Was auf Datenschutz spezialisierte Berater wie DSGVO-Referent Lambert Gneisz bedauern, ist, dass das Thema von vielen Betroffenen als reine Schikane gesehen wird: „Die Maßnahmen aus der DSGVO bringen durchaus positive Effekte, die in die kaufmännische Betrachtung integriert werden sollten. Was wie stark zum Tragen kommt, hängt vom Unternehmen ab. Von besserer IT-Sicherheit, günstigeren Kosten durch bessere Prozesse über ein besseres Image nach außen bis hin zu motivierteren Mitarbeitern ist viel möglich.“ Gneisz erzählt, dass seine Kunden, wenn sie mit diesem Projekt durch sind, meist happy sind. Manche haben ihre Kundendatenbank endlich ausgemistet, andere sind gar auf neue Geschäftsideen gekommen, und die Musterschüler trauen sich sogar, mit ihren DSGVO-Maßnahmen Werbung zu machen. T

SERVICE

WER IHNEN BEI DER DSGVO HELFEN KANN

Ausgewählte Events und Initiativen.

→ Die nationale Datenschutzbehörde informiert unter der Rubrik „Europa & Internationales“ über die DSGVO und bietet auch einen laienverständlichen Leitfaden an. ***dsb.gv.at***

→ AK Wien, ÖAMTC, Microsoft, die Casinos u. a. haben sich im Verein Privacy Officers zusammengeschlossen, um sich bei der Umsetzung gegenseitig zu unterstützen. ***privacyofficers.at***

→ Ein Riesenthema ist die DSGVO bei der Wirtschaftskammer, die vor allem für KMU und EPU am laufenden Band DSGVO-Workshops in ganz Österreich abhält. Sehr rasche Anmeldung ist empfehlenswert, die Termine sind schnell ausgebucht. Gefördert werden auch externe Beratungsleistungen. Zudem hat die Kammer Datenschutzberater ausgebildet und bietet die wichtigen Dokumentvorlagen als Download an: ***wko.at/datenschutz***

→ Die ARGE Daten hält laufend Seminare zu unterschiedlichen Schwerpunkten der DSGVO. Auch hier gilt, sich rasch anzumelden, die meist eintägigen Seminare sind sehr gut gebucht: ***argedaten.at***

→ Der Gehalt der schier zahllosen Informationsvideos (Webinare) im Netz ist überschaubar und sehr redundant. Meist wird nur an der Oberfläche gekratzt. Um sich ein Bild zu machen, wie die DSGVO im eigenen Fall umgesetzt wird, empfiehlt sich vor allem der Austausch mit Branchenkollegen und dem Mitbewerb. Über die juristischen Konsequenzen auf das eigenen Geschäftsmodell klärt am besten der eigene Anwalt auf: Vereinbaren Sie rasch Termine, die Kapazitäten sind stark ausgelastet.

ZUSTIMMUNG EINHOLEN. Bestehende Newsletter-Abonnenten erneut um Zustimmung zu bitten, ist eine Option.

FOTOS: MICHAEL RAUSCH-SCHOTT, STUDIO HUGER