KLAUS JARITZ IM EXKLUSIV-INTERVIEW: DIE NEUE DSGVO AUF VERSTÄNDLICH

„Don't Panic!"

... meinte schon Schriftsteller Douglas Adams in seinem berühmten Roman „Per Anhalter durch die Galaxis". Ähnlich unüberwindbar wie eine Reise durch die Galaxie, scheint auf den ersten Blick auch die Umsetzung der neuen, ab Mai 2018 geltenden EU-Datenschutzgrundverordnung. Klaus Jaritz, GF der Hillside IT consulting GmbH und mittlerweile „Experte" in Sachen DSGVO, erklärt im E&W-Exklusivinterview was die neue Verordnung für (kleine und große) Unternehmen bedeutet - und zwar verständlich. Er beruhigt und rät: „Don't Panic! Die DSGVO ist keine Rocket-Science. Denn in Wahrheit müssen sich Unternehmer ihre Systeme nur ein einziges Mal hinsichtlich gespeicherter persönlicher Daten anschauen, das Prozedere im Kopf durchspielen und dokumentieren."

elektro.at via **STORYLINK: 1709010** **TEXT:** Stefanie Bruckbauer | **FOTOS:** K. Jaritz, D. Schebach, A. Morlok/ pixelio.de | **INFO:** www.hillside.at

Klaus Jaritz, GF der Hillside IT Consulting bringt die neue DSGVO im E&W-Exklusivinterview für jedermann verständlich auf den Punkt.

Klaus Jaritz ist Chef der Hillside IT consulting GmbH, einem Beratungsunternehmen mit Sitz in Kärnten, das sich darauf konzentriert, die IT Abteilungen in Unternehmen bei ihrer „teilweise etwas leidigen Strukturierungsarbeit", wie Jaritz (mit einem Zwinkern) formuliert, zu unterstützen. Das (heute 22-köpfige) Hillside-Team beschäftigt sich seit mehr als zehn Jahren mit IT-Sicherheit. Im Jahr 2016 kam als Teilbereich bzw Spezialthema die DSGVO, also die Datenschutz-Grundverordnung hinzu und in der Folge zwei Rechtsexpertinnen ins Team, die sich nur damit beschäftigen. Der Kärntner erläutert: „Die Datenschutz-Grundverordnung wurde bereits 2016 beschlossen – und schon viel früher diskutiert. Wir wissen also schon seit einiger Zeit was diesbezüglich auf uns zukommen wird und konnten uns vorbereiten. Aktuell befinden wir uns in der zwei Jahre dauernden Übergangsfrist. Diese endet am 25. Mai 2018."

„Das Datenschutzthema gibt es in Österreich im Grunde schon lange", berichtet der Hillside GF. „Wir haben mit dem DSG2000 ja ein existierendes (allerdings rein nationales) Datenschutzgesetz. Es wurden jedoch nie nennenswerte Strafen verhängt. Die mögliche Höchststrafe von 25.000 Euro zahlten die Betroffenen quasi aus der Portokassa und auf Grund dessen war es den Leuten, auf gut Deutsch, wurscht."

ALLES ANDERS

Das wird mit der DSGVO nun anders. Der Strafrahmen wurde „signifikant" erhöht, mit dem Ziel richtig schmerzhaft zu sein. So sind nun Strafen bis zu 20 Millionen Euro bzw 4% des Konzernumsatzes möglich. Jaritz geht allerdings davon aus, dass diese absurden Höchststrafen nur in besonders schweren Fällen verhängt werden: „Ein Unternehmen müsste dann schon grob fahrlässig und vielleicht sogar vorsätzlich gehandelt haben, zB indem Profiling im großen Stil betrieben wurde, sodass die Höchststrafe geltend wird. Dennoch: Die Strafen werden in jedem Fall unangenehm gestaltet sein. Für einen kleinen Elektrohändler können (Hausnummer) 50.000 Euro Strafe richtig weh

HILLSIDE IT CONSULTING

Die Hillside IT consulting ist ein Beratungsunternehmen mit Sitz in Kärnten. Zum Kerngeschäft zählen IT-Controlling, IT-Servicemanagement und IT-Sicherheits- bzw Risikomanagement. Zum Sicherheits- bzw Risikomanagement zählt im weitesten Sinne auch das Spezialthema DSGVO, also die neue EU Datenschutz-Grundverordnung. Hillside GF Klaus Jaritz beschäftigt 22 Mitarbeiter – darunter zwei Rechtsexpertinnen, die sich auf die DSGVO spezialisiert haben. Die Hillside IT consulting ist österreichweit sowie im Süden Deutschlands tätig und betreut derzeit rund 110 Unternehmen.

KONTAKT HILLSIDE IT CONSULTING
Adi-Dassler-Gasse 2, 9073 Klagenfurt
Tel: +43 (0) 463 / 292617
Mail: klaus.jaritz@hillside.at

Dieses Interview ist aus Sicht eines Praktikers und NICHT als verbindliche Rechtsauskunft zu sehen.

DES PUDELS KERN

Die DSGVO hat das Ziel das Datenschutzrecht in Europa zu vereinheitlichen und den EU-Bürger zu schützen.

-) Der Bürger hat künftig mehr Sicherheit und Kontrolle über seine Daten.
-) Der Bürger hat das Recht (und nun auch die entsprechend Macht in Form der DSGVO hinter sich) Unternehmen in Form eines „Auskunftsbegehrens" zu fragen, welche Daten von ihm gespeichert sind und was damit passiert.
-) Das betroffene Unternehmen muss innerhalb der vorgeschriebenen Zeit von einem Monat eine „entsprechend genormte" Antwort geben.
-) Hat das Unternehmen über diesen Bürger falsche Daten oder grundlos gespeicherte Daten („ohne Rechtsgrund"), dann kann dieser die Löschung oder Änderung der Daten verlangen.

BEISPIEL

Wenn ein Kunde fragt, welche persönlichen Daten gespeichert werden, muss man als Unternehmen den „Rechtsgrund" erläutern: Ich habe Deine Namensdaten, weil du mein Kunde bist und wir in einem Vertragsverhältnis stehen. Ich habe Adressdaten, damit ich Dir ein Produkt, dass Du bei mir im Webshop bestellst, schicken kann. Ich sammle Deine Bonitätsdaten, weil ich oft große Projekte für Dich abwickle, etc...

tun." Schlussendlich werde das Strafmaß im Ermessen der Richter liegen, abhängig von etwaigen Milderungsgründen, wie Jaritz meint, laut dem das übrigens nur einer von vielen Punkten in der neuen DSGVO sei, bei dem man die Rechtssprechung abwarten müsse.

DES PUDELS KERN

Was sich dem „Otto-Normalbürger" aus dem Gesetzestextkauderwelsch nicht gleich erschließt, ist das elementare Ziel der neuen Verordnung - also quasi des Pudels Kern. Jaritz bringt es verständlich auf den Punkt: „Es geht im Grunde um die Vereinheitlichung des Datenschutzrechtes innerhalb Europas. Künftig sind in allen EU-Staaten die gleichen Datenschutzpflichten und -rechte gültig (womit verhindert wird, dass es innerhalb Europas ‚Rückzugsräume' im Bereich Datenschutz gibt.) Die neue DSGVO trifft alle Unternehmen egal welcher Größe in Europa bzw., die in Europa Geschäfte machen. Im Mittelpunkt steht dabei der einzelne Bürger. Dieser soll geschützt werden und mehr Sicherheit bzw Kontrolle über seine Daten haben."

Das Ganze funktioniert ab 25. Mai 2018 wie folgt: Jeder Bürger kann egal welchem Unternehmen ein so genanntes „Auskunftsbegehren" schicken und in dieser Form fragen, welche persönlichen Daten von ihm zu welchem Zweck wie lange gespeichert werden. „Also, fragen konnte man früher auch schon, aber ab 2018 hat man als Bürger das Recht und in Form der DSGVO auch die entsprechende Macht hinter sich", so Jaritz, der das grundsätzlich gar nicht schlecht findet, denn: „Viele Leute (auch ich) surfen oft relativ unkontrolliert im Netz, laden Apps herunter oder registrieren sich irgendwo. Mich persönlich würde bei manchen Unternehmen schon sehr interessieren, welche Daten sie von mir im Laufe der Zeit gesammelt und gespeichert haben."

Trudelt bei einem Unternehmen ein Auskunftsbegehren ein, dann muss dieses in der gesetzlich vorgeschriebenen Zeit von einem Monat eine entsprechend genormte Antwort geben. „Entsprechend genormt", heißt: Die DSGVO gibt vor, wie Unternehmen den Verbraucher beauskunften müssen, wie die Antwort auf so ein Auskunftsbegehren also auszusehen hat. Jaritz geht davon aus, dass alle diese Formvorschriften in Zukunft im Internet zwecks Download zur Verfügung gestellt werden. *(Auf elektro.at finden Sie u.a. - als Beispiel wie so etwas aussehen könnte - die Vorlage für ein Auskunftsbegehren. Dieses Formular gilt allerdings für das DSG-2000, also für das gegenwärtige, „alte" Datenschutzgesetz. Für die neue DSGVO gibt es noch kein Template. Sobald vorhanden wird es von der Datenschutzbehörde veröffentlicht. Jaritz geht davon aus, dass es sich nicht viel von dem jetzigen unterscheiden wird.)*


© Dominik Schebach

Hat das Unternehmen, das mit einem Auskunftsbegehren konfrontiert wird, Zweifel an der Identität des Fragenden, dann muss diese nachgewiesen werden – zB in Form einer Ausweiskopie. Jaritz ergänzt: „Wenn das Auskunftsbegehren beispielsweise über eine Fantasiemailadresse oder telefonisch erfolgt, dann kann das Unternehmen Informationen zur Bestätigung der Identität anfordern. Sonst könnte ich, Klaus Jaritz, ja ganz einfach herausfinden, welche persönlichen Daten von Steffi Bruckbauer bei der motopress gespeichert sind."

„Die DSGVO umfasst unzählige Details, die kleine Unternehmen allerdings nicht unbedingt betreffen."

Klaus Jaritz

DIE RICHTIGE ANTWORT

Um antworten zu können, muss man wissen WO im Unternehmen Kundendaten gespeichert sind. Jaritz: „Für kleine Unternehmen wird das kein Problem sein. Ein kleiner Elektrohändler wird in den fünf im Büro stehenden Computern einfach nachschauen, wo welche Daten gespeichert sind." Bei großen Unternehmen - und da zieht das Gesetz eine Trennlinie - ist die Situation anders: Ab 250 Mitarbeitern (unter ganz besonderen Umständen und bei hohem Risiko „für Recht und Freiheiten der Privatperson" auch in kleineren Unternehmen) muss nämlich ein so genanntes Verarbeitungsverzeichnis geführt werden. Darin muss dokumentiert werden, woher die Daten über Personen stammen, wo sie in welcher Form aufgehoben werden, zu welchen Zwecken sie verarbeitet werden und was damit passiert. Dieses Verarbeitungsverzeichnis kann geprüft werden und unterliegt auch gewissen gesetzlichen Formvorgaben.

Ein Verarbeitungsverzeichnis ist wie soeben erläutert zwar erst ab einer Größe von 250 Mitarbeitern (und unter besonderen Umständen auch kleiner) gesetzlich vorgeschrieben, bei Firmen mit beispielsweise 120 Mitarbeitern und dementsprechend vielen Systemen würde es sich Jaritz' Meinung nach aber auch schon auszahlen: „Es würde genügen eine Excel-Tabelle mit den ‚richtigen Kategorien' anzulegen, also mit mehreren Spalten für Art, Zweck, Dauer, Weitergabe, etc aller Kundendaten, weil dann gibt es einen zentralen Ort, an dem man nachschauen kann. Der Initialaufwand ist eingangs freilich etwas höher, auf der anderen Seite ist es dann um ein Vielfaches leichter, wenn wirklich eine Anfrage eintrudelt."

Hat der Kunde schließlich eine Antwort auf sein Auskunftsbegehren bekommen, ist er entweder zufrieden und

EU-GESETZ VS. VERORDNUNG

Meistens läuft es wie folgt: Im Bestreben, wichtige Rechtsgebiete im Spannungsfeld zwischen Wirtschaft und Verbraucher zu harmonisieren, baldowert die EU-Kommission in Brüssel ein Gesetz aus. Dieses wird dann noch ausführlich diskutiert, mehrfach geändert und schließlich vom EU-Parlament verabschiedet. Danach bekommen die 28 Mitgliedstaaten eine Frist gesetzt, innerhalb derer sie diesen Beschluss in nationales Recht überführen müssen. Erst dann müssen sich Unternehmen in den einzelnen Ländern wirklich darum kümmern.

Bei der EU-Datenschutz-Grundverordnung läuft es anders. Die DSGVO ist nämlich kein Gesetz, sondern eine Verordnung. Deshalb muss sie auch nicht in nationale Gesetze gegossen werden, sie tritt einfach in Kraft, und zwar am Freitag, den 25. Mai 2018.

BEGRIFFSERKLÄRUNG

Auskunftsbegehren - Jeder Bürger kann ein Unternehmen in Form eines „Auskunftsbegehrens" fragen, welche persönlichen Daten von ihm zu welchem Zweck (wie lange) gespeichert werden.

Datenschutzfolgeabschätzung - Diese ist durchzuführen, wenn besonders sensible Daten verarbeitet werden. Sie dient der Bewertung von Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der Betroffenen.

Einverständniserklärung - Kunden und Mitarbeiter müssen der Speicherung ihrer Daten zustimmen. Formulierungsvorschlag: „Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich ... (Datenarten, zB Name, Adresse, ...) zum Zweck der ... (Zweckangabe, zB „Zusendung von Werbematerial über die Produkte der Firma...") gespeichert und verarbeitet werden."

Informationspflicht - gehen sensible Daten „verloren", dann müssen die Betroffenen („unverzüglich") und die Datenschutzbehörde (innerhalb von 72 Std.) davon in Kenntnis gesetzt werden.

Personenbezogene Daten - alle Informationen, die sich auf eine identifizierbare, natürliche Person beziehen. zB Name, Adresse, Geburtsdatum, Bankdaten, etc.

Profiling - jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten; insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Rechtsgrundlage - Aus welchem Grund/zu welchem Zweck werden persönliche Daten gespeichert.

Sensible personenbezogene Daten - Informationen über rassische, ethnische Herkunft, politische Meinungen, religiöse, weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, biometrische Daten, genetische Daten, Angaben zum Sexualleben, sexuelle Orientierung.

Verarbeitungsverzeichnis - Ist die Dokumentation aller Verarbeitungstätigkeiten in denen personenbezogene und/oder sensible Daten verarbeitet werden. Dokumentiert werden müssen: der Zweck der Verarbeitung, Kategorien betroffener personenbezogener Daten, Kategorien betroffener Personen, Empfänger der Daten, Speicherfrist und die technischen sowie organisatorischen Maßnahmen, die unternehmensintern für den Schutz getroffen wurden.

man hört nichts mehr von ihm. Oder er stellt einen Antrag auf Änderung bzw Löschung der Daten. Dieses Prozedere (also das Auskunftsbegehren des Kunden, die Antwort des Unternehmens und allfälliges Ändern oder Löschen der Daten) sollte dabei unternehmensseitig dokumentiert werden, damit man die getätigten Schritte im Fall der Fälle belegen kann. Jaritz wirft einen wichtigen Aspekt ein: „Als Unternehmen wird man erst dann mit diesem Prozedere konfrontiert, wenn man das erste Auskunftsbegehren in Händen hält. Bekommt ein kleiner Elektrohändler, als Beispiel, also nie ein Auskunftsbegehren geschickt, dann wird er sich auch nie mit dieser Thematik beschäftigen müssen."

ZUSTIMMUNG

Spätestens ab 25. Mai 2018 brauchen Unternehmen eine Einverständnis- bzw-Zustimmungserklärung ihrer Kunden, wenn Daten gespeichert werden sollen. Das betrifft vor allem im Internet tätige Unternehmen, wie zB Elektrohändler mit Webshop. „Wenn ein Kunde im Ladengeschäft kauft, gibt er im Normalfall keine Daten preis. Und wenn doch, weil man ihm zB eine Gerätegarantie verkauft und dafür Name und Anschrift benötigt, dann muss die Zustimmungserklärung auf Papier erfolgen. Am besten in Form eines Passus auf dem Garantieformular („Ich erkläre mich einverstanden, dass meine Daten ...)", wirft Jaritz ein.

> „Wir haben ja ein existierendes Datenschutzgesetz. Es wurden jedoch nie nennenswerte Strafen verhängt (...) und auf Grund dessen war es den Leuten, auf gut Deutsch, wurscht."
>
> Klaus Jaritz

Was die Zustimmungserklärung betrifft, müssen sich Unternehmen im Vorfeld überlegen, welche Daten für welche Zwecke gespeichert werden sollen. Nach dem Datenschutzgesetz dürfen Daten nämlich nur für „festgelegte, eindeutige und rechtmäßige" Zwecke ermittelt und nur „nach Treu und Glauben und auf rechtmäßige Weise" verwendet werden. So ist zB die Speicherung von Daten zwecks Durchführung krimineller Machenschaften (klarerweise) unzulässig. Rechtmäßig wäre hingegen die Datenspeicherung zB für den Zweck der Auftragsverwaltung oder Buchhaltung. Jaritz empfiehlt: „Als Webshopbetreiber sollte man irgendwo gut sichtbar den Satz einbinden ‚Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich ... (Name, Adresse, ...) zum Zweck der ... (zB Zusendung von Werbematerial über die Produkte der Firma...) gespeichert und verarbeitet werden.' Der Kunde muss dann zwecks Zustimmung ein Hakerl anklicken." Aber Achtung: Leitet das Unternehmen die Daten zB an eine Bank zwecks Bonitätsauskunft weiter, dann MUSS diese mögliche „Übermittlung an Dritte" in der Einverständniserklärung angeführt sein. Der Kunde muss also schon beim „Unterzeichnen" der Einverständniserklärung wissen, dass seine Daten unter Umständen an Dritte übermittelt werden.

„SENSIBLER" SPEZIALFALL

Klarerweise muss man als Unternehmer auch eine Einverständniserklärung von seinen Mitarbeitern (die wie alle EU-Bürger das Recht auf Kontrolle und Sicherheit ihrer Daten haben), einholen. Das ist deshalb so wichtig, da man von seinen Angestellten nicht nur persönliche Daten, wie Name, Anschrift, Geburtsdaten, etc, speichert, sondern in der Regel auch „sensible Daten". Dabei handelt es sich um Informationen über rassische, ethnische Herkunft, politische Meinungen, religiöse, weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, sexuelle Orientierung, etc. Jaritz dazu: „Jedes Unternehmen, das Angestellte beschäftigt, hat mit allerhöchster Wahrscheinlichkeit irgendwelche sensiblen Daten, wie u.a. Religionszugehörigkeit oder Gesundheitszeugnisse, gespeichert. Wenn diese Daten verloren gehen bzw ‚veröffentlicht' werden, dann müssen die betroffenen Personen darüber informiert werden (=Informationspflicht). Auch die Datenschutzbehörde muss vom Verlust sensibler Daten in Kenntnis gesetzt werden und zwar innerhalb von 72 Stunden."

Was sensible Daten angeht, muss man sich als Unternehmer bereits im Vorfeld überlegen, was es bedeutet, wenn diese verloren gehen. „Man sollte eine Art Risikoabschätzung durchführen, das ist in der DSGVO ein Formalprozess und wird Datenschutzfolgeabschätzung genannt. Unter gewissen Umständen muss ein Unternehmen der Datenschutzbehörde auch melden, welche sensiblen Daten wo gespeichert sind und wie diese abgesichert werden. Das betrifft im Normalfall aber keinen Elektrohändler, sondern eher zB ein Krankenhaus, das ja nahezu ausschließlich sensible (Gesundheits-)Daten speichert."

ALLES SO KOMPLIZIERT

Wie Jaritz empfiehlt, sollte sich jeder Unternehmer, egal wie klein oder groß, einmal gut überlegen: Welche Daten habe ich über meine Kunden in welchem System (Computer, externe Festplatten, Kundenkarteisysteme, Excel, Outlook, etc) gespeichert? Warum habe ich diese

Daten und was mache ich damit? Übermittle ich sie zB an Dritte? „Das klingt jetzt furchtbar kompliziert, ist es aber nicht“, so Jaritz, „denn in Wahrheit muss ich mir meine Systeme nur ein einziges Mal hinsichtlich gespeicherter persönlicher Kundendaten anschauen. Finde ich dabei Daten, die ich nicht mehr brauche oder hinter denen kein existierender Rechtsgrund mehr steht, sollte ich sie löschen. Wir haben zB Fälle von Vertriebsmitarbeitern, die rein aus guter Absicht Informationen über ihre Kunden sammeln und speichern. So zB welche Hobbies und Vorlieben der Kunde hat, damit man ihn auch einmal mit einer Nettigkeit (zB einem Flascherl Rotwein, weil er den so gerne trinkt) überraschen kann. Derartige Sammelleidenschaften könnten künftig allerdings unter Profiling fallen und für dieses ist eine ausdrückliche Einwilligung der betroffenen Person nötig.“

Der Kärntner entwarnt: „Es ist zum jetzigen Zeitpunkt davon auszugehen, dass die Datenschutzbehörde erst dann tätig wird, wenn es zu einem Verstoß kommt und dieser gemeldet wird. Wenn man auf ein Auskunftsbegehren zB gar nicht oder sichtlich nur Blödsinn antwortet. Oder wenn Daten trotz Aufforderung nicht gelöscht werden.“

SCHRITT FÜR SCHRITT

Unternehmen aller Größen sollten nun wie folgt vorgehen, um sich auf die DSGVO vorzubereiten:

Systeme durchforsten, Überblick schaffen:
-) Wo im Unternehmen liegen Daten?
-) Um welche Daten handelt es sich und wie lange darf man sie behalten?
-) Was mache ich mit diesen Daten?
-) Gebe ich Daten an Dritte weiter?
-) Betreibe ich mit diesen Daten Profiling? Jaritz erklärt: „Auf kleine Elektrohändler wird Letzteres nicht zutreffen, wobei es würde schon reichen, wenn ich aus meinen Kundendaten alle Personen im Alter von 20- und 30 Jahren, die in Wien wohnen und bei mir einen Samsung-TV gekauft haben, raussuche und mit diesen Informationen etwas mache (zB abgestimmte Kaufentscheidungen). Dieses Profiling ist per se nicht verboten, man benötigt allerdings, wie schon erwähnt, eine nachweisbare ausdrückliche Einverständniserklärung der betroffenen Person dafür.“

> „Das klingt jetzt furchtbar kompliziert, ist es aber nicht.“
>
> Klaus Jaritz

Einverständniserklärung? Unternehmen sollten sich überlegen, wie sie künftig zu einer Einverständniserklärung seitens ihrer Kunden und Mitarbeiter für die Speicherung von Daten kommen. Jaritz ergänzt: „Diese Formulierungen muss man nicht selbst erfinden. Bald werden diverse Institutionen, wie zB die WKÖ, Vorlagen zur Verfügung stellen.“

Datenschutzfolgeabschätzung? Unternehmen sollten zudem überlegen, ob sensible Daten gespeichert sind, die nach einer Datenschutzfolgeabschätzung verlangen und (wenn ja), ob technische Aktionen zu setzen sind (zB ein Verschlüsselungssystem in der IT einführen). Um das mit Sicherheit beantworten zu können, sollte ein Experte bzw Rechtsanwalt zu Rate gezogen werden, wie Jaritz empfiehlt. Der Kärntner meint aber auch: „Ein kleiner Elektrohändler mit fünf Mitarbeitern wird wahrscheinlich keine Datenschutzfolgeabschätzung brauchen.“

Prozesse definieren: Als nächstes sollten sich Unternehmer überlegen, wie sie im Falle eines Auskunftsbegehrens, einer Änderungs- UND Löschanfrage vorgehen werden. „Diesen Vorgang muss man sich EIN Mal überlegen“, empfiehlt Jaritz. „Je größer das Unternehmen, desto eher sollte ein fixer Prozess festgelegt werden, welche Schritte zu tätigen sind. Größere Unternehmen werden auch noch ein paar andere Detailprozesse in Betracht ziehen müssen.“

UNZÄHLIGE DETAILS

„Die DSGVO umfasst unzählige Details, die kleine Unternehmen allerdings nicht unbedingt betreffen“, so der Hillside GF, der empfiehlt das ganze Prozedere einmal im „Trockentraining“ Schritt für Schritt durchzuspielen, sich vielleicht sogar ein Auskunftsbegehren zu besorgen und so zu tun als müsste man es beantworten. Bei unklaren Details wäre es empfehlenswert kurz einen Rechtsexperten zu Rate zu ziehen. Das alles sollte zudem niedergeschrieben werden. Diese Dokumentation der umgesetzten Prozesse innerhalb des Unternehmens ist einer der Eckpfeiler der DSGVO und wird man bei Gelegenheit auch vorweisen müssen.

Auf die Frage, was Klaus Jaritz von der DSGVO hält, meint der Hillside GF: „Auch wenn mich manche dafür prügeln wollen – ich finde die Verordnung grundsätzlich sinnvoll. In Europa herrscht viel zu wenig Bewusstsein für den Wert von Information. Es ist unglaublich wie freizügig und unüberlegt heutzutage Daten weitergegeben werden. Ich glaube, dass wir uns unseren Wettbewerbsvorteil innerhalb Europas nur dann erhalten können, wenn wir unsere Informationen und Daten auch schützen. In Zeiten von Geschäftsmodellen, bei denen Hacker Millionen von Daten illegal von Unternehmensservern saugen und verkaufen, muss man endlich beginnen gegenzulenken. Dieses Gegenlenken erzeugt klarerweise Aufwand und das tut keiner gerne, aber ganz ehrlich: wem tut es denn weh, wenn er sich EIN Mal überlegt, was für Daten er gespeichert hat. Eine sinnvolle Beschäftigung ist das allemal.“ ■

Die neue DSGVO birgt einige Punkte, bei denen man noch die Rechtssprechung abwarten muss.

FRAGEN, DIE SICH AUFDRÄNGEN

Was ist mit Daten, die man über die Jahre gesammelt hat? Daten, die ohne existierenden Rechtsgrund gespeichert sind, müssen gelöscht werden. Oder man holt vom Betroffenen eine Zustimmungserklärung ein.

Wie oft kann ein Kunde ein Auskunftsbegehren stellen? Ein Mal im Jahr „kostenlos“. Für alle weiteren Male, kann ein Unternehmen Geld verlangen.

Muss ein Unternehmen wegen der DSGVO die IT umstellen? Eher nein. Das Gesetz (das in diesem Punkt sehr schwammig ist) schreibt lediglich vor, dass die IT „state of the art“ sein sollte. Sensible Daten zu speichern und kein Backup-System zu haben, wäre zB NICHT state of the art.

Über die kommende Datenschutzklippe haben wir in der E&W 7-8/ 2017 bereits berichtet. Dabei erläuterte der anerkannte DSGVO-Rechtsexperte Dr. Rainer Knyrim im Interview die rechtlichen Grundlagen und Herausforderungen. Diesen Artikel und weitere Informationen zur DSGVO finden Sie, wenn Sie folgendem Storylink folgen ...

elektro.at bietet mehr Information via **STORYLINK: 1709010**

ARTIKEL : E&W 7-8/ 2017, Die Datenschutzklippe naht

DOWNLOAD : Formulare DSGVO