EU-DSGVO: Chancenreiches Damoklesschwert

von Rudolf Felser

Die Europäische Datenschutzgrundverordnung hängt wie ein Damoklesschwert über vielen Köpfen. Man kann sie aber auch als Chance sehen.

Wenn die EU-DSGVO am 25. Mai 2018 in Kraft tritt, ist die Schonfrist vorbei. Spätestens dann muss sie im Unternehmen umgesetzt sein. Wir haben Experten eingeladen, mit uns über dieses Thema zu diskutieren und es aus verschiedenen Blickwinkeln zu beleuchten. Unserem Ruf gefolgt sind Roman Hohl, Country Manager für Österreich und die Schweiz bei dem Cybersecurity-Anbieter Palo Alto Networks, Vincenz Leichtfried, selbständiger Unternehmer im Bereich Daten- und IT-Security und anwesend als Vertreter der WKÖ-Fachgruppe UBIT-Wien, der Rechtsanwalt Franz Lippe, bei Preslmayr Rechtsanwälte vorwiegend im Medien- und Datenschutzrecht tätig, Benigna Prochaska, Geschäftsführerin des 2017 gegründeten Unternehmens Intervalid, das sich auf die Entwicklung einer DSGVO-Software spezialisiert hat, Stefan Schachinger, technischer Leiter im Pre-Sales-Bereich für die Data-Protection-Produktsparte von Barracuda Networks in EMEA, sowie Gottfried Tonweber, Senior Manager bei EY und Leiter des Bereichs Cybersecurity & Data Privacy in Österreich.

Die DSGVO kommt, schnallen Sie sich an

Zu Beginn wurde das Missverständnis ausgeräumt, man könnte sich vor der EU-DSGVO drücken. Jurist Franz Lippe stellte klar: „Grundsätzlich zieht jede Form der Verarbeitung von personenbezogenen Daten die Anwendbarkeit der Datenschutzgrundverordnung nach sich. Deswegen kann jedes Unternehmen grundsätzlich davon ausgehen, dass die DSGVO anwendbar ist. Manche Unternehmen meinen, sie müssen keinen Datenschutzbeauftragten bestellen oder kein Verzeichnis von Verarbeitungstätigkeiten führen. Das mag sein, bedeutet aber noch lange nicht, dass die anderen Rechte und Pflichten nach der Datenschutzgrundverordnung sie nicht betreffen." Vincenz Leichtfried verdeutlichte mit einem Beispiel: „Es muss kein Hacker-Angriff sein, es reicht, wenn man das Smartphone liegen lässt, das Notebook gestohlen wird oder man versehentlich sorglos mit Daten umgeht, etwa eine E-Mail falsch versendet. Oft sind es die einfachen Dinge, die ein Auslöser für einen Verstoß sein können. Dann ist jeder betroffen und die Datenschutzbehörde kann an die Tür klopfen." Mit dem Beispiel der Einführung der Gurtpflicht in den 1970er-Jahren zeichnete Gottfried Tonweber ein klares Bild: „Heutzutage wird hoffentlich niemand daran zweifeln, ob es eine Gurtpflicht braucht und warum es sinnvoll ist, sich anzuschnallen. In einer digitalen Welt, die veränderte Geschäftsmodelle mit sich bringt, geht es darum, wie man analog zur Straßenverkehrsordnung ein Regelwerk für den Datenverkehr und Strukturen zum Schutz von Daten herstellt. Deswegen hat der Gesetzgeber die Datenschutzgrundverordnung auf EU-Ebene verordnet und deswegen geht sie alle an. An einen Bio-Bauern werden natürlich nicht die gleichen Anforderungen gestellt wie an einen internationalen Konzern. Aber auch der Bio-Bauer muss sich überlegen, inwiefern er betroffen ist und welche grundlegenden Tätigkeiten – beispielsweise ein Verfahrensverzeichnis – notwendig sind."

> „Jedes Unternehmen kann davon ausgehen, dass die DSGVO anwendbar ist."
>
> Franz Lippe,
> Preslmayr Rechtsanwälte

Welche Rolle spielt IT?

IT-gestützte Maßnahmen spielen eine wesentliche Rolle im DSGVO-Kanon, besonders im Kontext der IT-Sicherheit. Aber wie sieht diese Rolle aus? Das haben wir die Security-Anbieter gefragt. Stefan Schachinger dazu: „Im Gesetz werden keine konkreten Maßnahmen gefordert. Es heißt immer ‚der Stand der Technik'. Jedes Unternehmen sollte mit einer Erhebung beginnen, wo welche Daten verarbeitet werden. Man muss sich überlegen, wie diese Daten technisch gesichert sind und welche Risiken bestehen."

Die Teilnehmer des Round Tables von links nach rechts: **Roman Hohl,** Palo Alto Networks, **Vincenz Leichtfried,** UBIT-Wien, **Benigna Prochaska,** Intervalid, **Gottfried Tonweber,** EY, **Stefan Schachinger,** Barracuda Networks, **Franz Lippe,** Preslmayr Rechtsanwälte

Für Roman Hohl steht fest: „Die Anbieter haben alle das gleiche Ziel: es den Leuten, die an unsere Daten oder in unsere Infrastruktur möchten, schwieriger zu machen. Wichtige Themen sind in diesem Zusammenhang Automatisierung, um mit deren Geschwindigkeit mithalten zu können, und Prevention. Es sollte gar nicht so weit kommen, dass Sie jemanden in Ihrer Infrastruktur haben, denn dann wird die Abwehr schwierig. Das ist aber nicht nur ein Technologiethema, sondern auch ein Organisations- und Personenthema."

Während die einen versuchen, es den „Bösewichten" so schwer wie möglich zu machen, wollen andere wiederum Dinge erleichtern – wie eben die Umsetzung der „schwer verdaulichen" EU-DSGVO. Benigna Prochaska, die sich mit ihrem Unternehmen ebendieses Ziel gesetzt hat, erzählte: „Kleine Unternehmen kann man unterstützen, indem man das Thema greifbarer macht. Es gibt sehr viele Seminare, man hört viel Theorie, aber die praktische Umsetzung ist schwierig. Wie sieht so ein Verzeichnis aus? Welche Felder muss es haben? Hier kann man die Unternehmen mit Mustervorlagen und möglichst einfachen Strukturen unterstützen." Auch sie brachte das „Personenthema" aufs Tapet. Man müsse im Unternehmen eine Awareness für das Thema schaffen und möglichst viele Mitarbeiter an Bord holen. Denn: „Die Umsetzung kommt von den Mitarbeitern, denn sie haben mit den personenbezogenen Daten zu tun."

Der Datenschutz-Triathlon

Privacy-Experte Tonweber sprach einen ganz zentralen Punkt an: „Das Problem mit der Datenschutzgrundverordnung ist, dass man drei Aspekte zusammenbringen muss, die sonst nicht so viel miteinander zu tun haben: Es gibt eine Rechtsperspektive, einen organisatorischen bzw. prozessualen Aspekt und einen Technik-Aspekt. Diese drei Themen erfordern eigentlich einen ‚Triathleten'. Die Datenschutzbeauftragten oder -verantwortlichen – je nachdem, was das Unternehmen benötigt – sind Manager, die bereichsübergreifend agieren und Recht, Prozess und Technik zusammenbringen müssen. Erfreulich ist, dass das Thema mittlerweile auf der Führungsebene angekommen ist. Der Gesetzgeber hat ganz bewusst hohe Strafen mit 4 Prozent des Umsatzes bzw. 20 Mio. Euro gewählt."

Roman Hohl bestätigte, dass das Thema auf der Ebene des C-Levels angekommen ist: „Wir sehen, dass die CISOs, die bisher irgendwo unter dem IT-Manager oder Finanzchef versteckt waren, jetzt direkt an die CEOs berichten. Das ist ein gutes Zeichen. Das zeigt, dass verstanden wird, worum es geht."

Ist noch genügend Zeit?

Anders als beispielsweise die Registrierkassenpflicht lässt sich die EU-DSGVO nicht im einfachsten Fall mit einem Tablet, einer App und einem Drucker lösen. Sie bedarf schon etwas mehr an Arbeit. Die Uhr tickt, bis Mai 2018 ist es nicht mehr lang. Tonweber beruhigte jedoch: „Die Frist ist zwar knapp bemessen. Aber wenn die KMUs, mit Fokus auf dem ‚K', sofort beginnen, können sie es schaffen. Was braucht man wirklich? Das Verfahrensverzeichnis muss sinnvoll erhoben werden und man muss sich überlegen, wo man die Funktion verortet. Braucht man einen Datenschutzbeauftragten oder eher nur einen -verantwortlichen? Bis Mai sind diese Grundlagen machbar. Wenn die Behörde das Gefühl hat, ein Unternehmen hat sich eingehend mit der Umsetzung beschäftigt, dann wird es auf breites Wohlwollen stoßen, gerade im KMU-Bereich." Leichtsinnigkeit ist Vincenz Leichtfried zufolge dennoch nicht angebracht: „Kleinere Unternehmen, die weniger Ressourcen haben und nicht einfach Top-Berater einstellen können, müssen sehen, wie sie mit ihren Ressourcen zurechtkommen. Jetzt kommt Weihnachten, der Jahresabschluss, und dann geht's erst richtig los. Dann werden wahrscheinlich auch die Berater schwer verfügbar sein, weil sie entsprechend ausgelastet sein werden."

Deswegen sollte man sich rasch an die Arbeit machen. Franz Lippe brachte die Vorgehensweise auf den Punkt: „Chronologisch gesehen ist der Anfang die Erhebung der Datenver-

Alle Teilnehmer des Round Tables waren sich einig, dass die EU-DSGVO nicht nur als Herausforderung, sondern auch als Chance gesehen werden sollte.

arbeitungstätigkeiten mit dem Ziel der Erstellung eines Verzeichnisses. Dieses Verzeichnis soll auch dazu dienen, zu sehen, welche Pflichten nach der DSGVO überhaupt auf das Unternehmen zukommen können – weil es beispielsweise sensible Daten verarbeitet oder die Zustimmung des Betriebsrates für eine gewisse Form der Verarbeitung von Mitarbeiterdaten braucht." Dann gibt es da noch die Benennung des Datenschutzbeauftragten. Lippe weiter: „Mit der Benennung des Datenschutzbeauftragten treffen mich gewisse Pflichten, auch aus dem Arbeitsrecht. Wenn ich einen Datenschutzverantwortlichen oder einfach jemanden im Unternehmen bestimme, der sich um das Thema Datenschutz kümmert, der aber kein Datenschutzbeauftragter im Sinne der Datenschutzgrundverordnung ist, habe ich auch keinen Datenschutzbeauftragten. Es muss jedenfalls jemanden geben, der sich mit dem Thema beschäftigt. Ob er aber als Datenschutzbeauftragter im Sinne der DSGVO benannt wird oder nicht, damit sollte man sich beschäftigen."

Es gibt also einen Unterschied zwischen dem Datenschutzbeauftragten und dem Datenschutzverantwortlichen. Diesen Unterschied erklärte Tonweber: „Der Datenschutzbeauftragte ist im Prinzip der Repräsentant der Datenschutzbehörde in Ihrem Unternehmen. Ähnlich wie ein Betriebsrat, der die Interessen der Arbeitnehmer vertritt, vertritt der Datenschutzbeauftragte die Interessen der Behörde. Der Datenschutzverantwortliche kümmert sich auch um den Datenschutz, aber ohne diesen rechtlichen Habitus. Leider gibt es keine genauen Vorgaben oder eine konkrete Mitarbeiterzahl als Grenze für die Notwendigkeit eines Datenschutzbeauftragten. Wenn der Hauptzweck der Kerntätigkeiten eines Unternehmens die umfangreiche Verarbeitung von sensiblen, personenbezogenen Daten ist, dann braucht man einen Datenschutzbeauftragten nach DSGVO. Wenn der Zweck nicht primär darin liegt, dann reicht ein Verantwortlicher."

Rechtsanwalt Lippe machte auf die Stolpersteine aufmerksam: „Da liegt der Hund begraben. Denn wenn ich mir den Text der DSGVO über die Fälle der Benennungspflicht ansehe, dann komme ich relativ schnell zu der Auffassung, dass auf mich keiner zutrifft, weil die Kerntätigkeit meines Unternehmens nicht in umfangreicher Datenverarbeitungstätigkeit liegt, sondern zum Beispiel im Fall eines Krankenhauses in der Krankenbehandlung. Aber die Artikel-29-Datenschutzgruppe vertritt in einem Working Paper die Meinung, dass Krankenhäuser ihre Kerntätigkeit – die Krankenbehandlung – nicht anders durchführen können, als durch umfangreiche Datenverarbeitung. Deswegen besteht die Kerntätigkeit eines Krankenhauses auch in der umfangreichen Verarbeitung von sensiblen Daten."

Umsetzungs-Tipps

Zum Abschluss haben wir in die Runde nach Tipps für die Umsetzung der EU-DSGVO gefragt. Hohl: „Man muss dem Thema Priorität geben. Man muss wissen, welche Daten man in der Infrastruktur hat, was man nutzt und wie man es nutzt. Ebenfalls ein Thema sind die Zugriffsrechte. Wenn heute jemand im Unternehmen seine Position wechselt, dann behaupte ich, dass 80 Prozent der Regeln nicht angepasst werden. Noch schlimmer ist es beim Remote Access. Wenn jemand die Firma verlässt, bin ich überzeugt, dass er sich auch nachträglich in Infrastruktur hängen kann. Das darf man nicht aus den Augen verlieren."

Leichtfried war der Ansicht, dass man die EU-DSGVO als Gelegenheit sehen sollte, das Datenmanagement und die Prozesse nach dem aktuellen Stand der Technik aufzustellen: „Wenn ich mir einen Datenmanager ins Unternehmen hole, der den Überblick hat, ist das eine Chance, mein Datenmanagement und meine Unternehmensprozesse besser zu gestalten."

Benigna Prochaska riet dazu, rechtzeitig mit den Softwareherstellern der eingesetzten CRM-, Buchhaltungs- oder HR-Software Kontakt aufzunehmen, „denn es gibt viele Dinge, die ich von der Software benötige, aber die vielleicht noch nicht bereitstehen – Protokollierung, ob die Daten gelöscht werden können, wie es erforderlich ist, ob man schnell Auskunft geben kann. Da ist man in einer Abhängigkeit von den Softwareherstellern." Ebenfalls nützlich ist es Prochaska zufolge, diese Prozesse, wenn man sie einmal beschrieben hat, durchzuspielen.

Einen sehr konkreten Hinweis gab Tonweber: „Wenn man sich das Datenverarbeitungsregister eines Unternehmens ansieht und es leer ist, kann man annehmen, dass dieses Unternehmen bisher nichts gemacht hat. Man sollte das DVR-Register, wenn es sich zeitlich ausgeht, noch befüllen. Auch, wenn es in Zukunft abgeschafft wird, denn das Datenverarbeitungsregister ist nichts anderes als das Verfahrensverzeichnis, das Unternehmen in Zukunft intern führen müssen. Wenn das DVR-Register leer ist, ist ein Unternehmen im Kontext der DSGVO relativ angreifbar. Jeder kann in das DVR-Register schauen, auch die Konkurrenz." Unterstützung erhielt er in dieser Hinsicht von Lippe: „Die Bedeutung des DVR darf nicht unterschätzt werden. Es wird der Datenschutzbehörde auch nach dem 25. Mai 2018 zu Dokumentationszwecken dienen und dafür bleibt es auch bis Ende 2019 online. Für die Datenschutzbehörde kann das DVR ein Punkt sein, anhand dessen sie entscheidet, welche Unternehmen kontrolliert werden. Deswegen sollte man auch jetzt noch Datenanwendungen beim DVR melden. Man ist nach derzeitiger Rechtslage dazu ja auch meist verpflichtet. Dazu kommt, dass Datenanwendungen, die ich beim DVR melde und die auch die Verarbeitung von sensiblen Daten umfassen, von der Datenschutzbehörde genau betrachtet werden. Wenn die Datenschutzbehörde auf eine solche Datenanwendung sozusagen ihr „Siegel" gibt, dann ist das für die DSGVO ein sehr positives Signal. Wenn nicht, dann weiß ich zumindest, was ich noch zu tun habe."

Security-Profi Schachinger sprach zum Abschluss ebenfalls von einer großen Chance: „Es geht um den Schutz unser aller personenbezogenen Daten. Wieder die Analogie zur Gurt- oder Helmpflicht: Die mögen damals als lästig angesehen worden sein, aber mittlerweile ist es eine Selbstverständlichkeit. Für Unternehmen sind das Erstellen des Verzeichnisses und der Überblick darüber, wo es Daten gibt, die gespeichert oder verarbeitet werden, auch die Auseinandersetzung mit dem Gesetzestext, eine Gelegenheit, intern zu entrümpeln und das, was übrig bleibt, angemessen technisch und organisatorisch zu schützen." ◻

Auf monitor.at/list/tag/round-table/ finden Sie das komplette Gespräch und weitere Round Tables zum Nachlesen.