Wenn die Datenschutzbehörde klingelt ...

Man kann den Ernstfall auch proben.

Foto: Pixabay / andibreit

Die im Vorjahr eingführte DSGVO erstreckt sich auf viele Bereiche in Unternehmen

Manfred Kainz. Auch wenn die Corona-Krise momentan alles überdeckt, bleiben profane Dinge trotzdem „am Tisch". Für die Versicherungs- und Finanzberaterbranche etwa die Frage „Die Datenschutzbehörde klopft an. Worauf muss ich vorbereitet sein?" Diese Herausforderung abseits des täglichen Geschäftes war Thema eines Webinars der Austrian Financial & Insurance Professionals Association (kurz AFPA), das ist der Branchenverband der selbständigen Versicherungsvermittler und Finanzberater Österreichs.

Die „Lotsin für Datenschutzrecht und praktische DSGVO-Umsetzung" in der AFPA, **Birgit von Maurnböck**, ist eine auf Datenschutzrecht spezialisierte Juristin und als Unternehmensberaterin für die Themen Datenschutz, Compliance und IT tätig. Sie hat bereits etliche Verfahren vor der Datenschutzbehörde (in weiterer Folge: DSB) auf Unternehmensseite begleitet. Bei dem Webinar ging sie daher auf praktische Fragen ein.

Was bisher geschah …
Oft führen Beschwerden von Betroffenen oder auch Mitbewerbern zu einer Prüfung - zum Beispiel aus dem Grund, weil der Betroffene meint, seine Betroffenenrechte seien nicht rechtskonform erfüllt worden. Bisher waren und sind mehrere tausend Verfahren in Österreich anhängig. Auch wenn die bisherigen Strafen meist nicht sehr hoch gewesen seien (mit Ausnahme der Österreichischen Post), gelte: „Unwissenheit schützt vor Strafe nicht", wie Maurnböck warnt. Natürlich leitet die Datenschutzbehörde auch amtswegig Verfahren ein, wenn sie z. B. aufgrund der Meldung einer Datenpanne den Verdacht hegt, dass in einem Unternehmen DSGVO und DSG nicht eingehalten werden.

Es beginnt mit Briefen
Grundsätzlich meldet sich die DSB schriftlich (an): mit einer „Aufforderung zur Stellungnahme" zu einer ihr zugegangenen Beschwerde. Nun gilt es, die dort formulierten Vorhaltungen genau zu prüfen, sicherheitshalber die Datenverarbeitung des betreffenden Beschwerdeführers einzuschränken, und innerhalb der Antwortfrist schriftlich Stellung zu nehmen.

Wenn man vielleicht wirklich Verabsäumtes auch gleich ausbessert, könne die DSB von Strafe absehen. Ebenso kann man der DSB natürlich Argumente vorbringen, warum man meint, rechtskonform gehandelt zu haben, vor allem, wenn es um Graubereiche aufgrund der noch sehr jungen DSGVO-Auslegung gibt.

Einschauen
Die DSB kann Einschau in das Verarbeitungsverzeichnis verlangen und erfragen, wie viele und welche Verantwortliche, Verarbeitungen und Auftragsverarbeiter (Vertragsvollständigkeit!) es gibt und ob Datenschutzfolgeabschätzungen durchgeführt wurden. Sie kann sich auch einzelne Verarbeitungen vorführen lassen und die Schulung der Mitarbeiter überprüfen.

Eine Datenschutzfolgenabschätzung muss man verpflichtend machen, wenn mindestens zwei der folgenden Kriterien zutreffen: Umfangreiche Verarbeitung besonderer Datenkategorien (Gesundheitsdaten, Religion etc.), umfangreiche Verarbeitung strafrechtsbezogener Daten, Erfassung von Standortdaten, Verarbeitung von Daten schutzwürdiger Personen (Personen unter 14 Jahren, Arbeitnehmer, Patienten); Zusammenführung bzw. Abgleich von Daten aus mehreren Verarbeitungen zu unterschiedlichen Zwecken, wenn die betroffenen Personen diese Verarbeitung üblicherweise nicht erwarten können, und wenn die Daten nicht direkt bei der betroffenen Person erhoben wurden.

Vor-Ort-Schwächen
Weiters kann die DSB bei einem höchstpersönlichen Besuch im Unternehmen selbst EDV-Systeme, die Zutritts- und Zugangsmöglichkeiten, die Papierablage (wer hat worauf Zugriff?), oder auch die Umsetzung und Einhaltung der TOMS kontrollieren.

Einen praktischen Tipp zur Vorbereitung auf einen DSB-Besuch hat Maurnböck noch: „Den Ernstfall proben!" Also etwa eine unangekündigte Prüfung durch qualifizierte Dritte (Auditoren) durchspielen lassen, regelmäßig interne Überprüfungen und Mitarbeiterschulungen machen und dokumentieren - aus Fehlern lernen und Fehlendes umgehend vervollständigen.

Österreich schützt sich zu wenig vor Gefahren im Internet

Red./ks. „Um das Ansteckungsrisiko mit dem Coronavirus zu senken, verbringen derzeit die Menschen einen großen Teil ihrer Freizeit im Internet. Leider nutzen Betrüger gerade jetzt die Zeit, um sich zu bereichern", warnt Helvetia-Österreich-Chef **Thomas Neusiedler** in einer Aussendung. Er unterlegt das mit einer aktuellen Studie, die im Auftrag von Helvetia Österreich im April unter 500 Personen zum Thema „Cyberattacken" durchgeführt wurde.

Internetnutzung während Corona
Zu den häufigsten Dingen, die zuletzt im Internet erledigt wurden, zählen das Bearbeiten von E-Mails und das Surfen - das tun neun von zehn Österreichern täglich oder zumindest mehrmals pro Woche. Soziale Medien werden von mehr als drei Vierteln rege genutzt. Darauf folgt die Information via Nachrichten- und Websites. Fast sechs von zehn Österreichern halten täglich oder mehrmals pro Woche Kontakt zu anderen über Videokonferenz-, Chat-Tools und -Apps. Online-Banking nutzt hingegen nur jeder Zweite laufend. „Online-Shopping ist - ganz entgegen dem vorherrschenden Gefühl - kein so weit verbreiteter Zeitvertreib: Nur 15 % shoppen häufig Kleidung, Elektronik und dergleichen. Einkäufe des täglichen Bedarfs wickeln nur 13 % mehrmals wöchentlich online ab", so Neusiedler.

Wachsamkeit und kritischer Umgang
Doch wie schützen sich Österreicher bei dem derzeit starken Internet-Traffic? Viele gaben an, keine Links zu dubiosen Seiten oder E-Mails im Spam-Ordner zu öffnen. Eine Mehrzahl sagte, auf einen kritischen Umgang mit sensiblen Daten zu setzen. Auch der private Finanzbereich wird offensichtlich als verletzlich gesehen: Knapp 60 % der Befragten gaben an, sich mit regelmäßigen Kontrollen der Kontoauszüge vor Cyberkriminalität zu schützen. „Ein Angriff muss aber keine unmittelbare Auswirkung auf das Bankkonto haben", gibt der Helvetia-CEO zu bedenken. „Internetbetrüger haben sensible Daten aller Art im Visier. Neben finanziellen Schäden können sie damit auch Identitäten stehlen, Unternehmen erpressen oder Menschen stalken."

Passwort- und Antivirenschutz vernachlässigt
Beim Einsatz „starker" Passwörter und der Nutzung von Antivirensoftware hat Österreich starken Aufholbedarf: Nur die Hälfte hat einen aktuellen Antivirenschutz; ein etwas höherer Anteil (55 %) setzt alles daran, möglichst sichere Passwörter zu verwenden. „Besonders erschreckend ist, dass nur die Hälfte der Befragten eine Antivirensoftware installiert hat, obwohl diese häufig kostenlos verfügbar ist", sagt Neusiedler. Zu den sonstigen Maßnahmen, mit denen sich die Befragten vor Cyberkriminalität schützen, zählt auch die Beschränkung der Sicherheitseinstellungen bei Social-Media-Accounts, die immerhin ein Drittel durchführt. Nur ein Viertel der Befragten nutzt dagegen VPN/Verschlüsselung in öffentlichen WLANs und informiert sich aktiv über Datenpannen und Betrugsmaschen im Internet. Knapp 5 % schützen sich gar nicht und nur etwas mehr als 3 % der Befragten gaben an, eine Cyberversicherung zu haben. „Eine Cyberattacke kostet im Schnitt mehrere tausende Euro pro Schadensfall, was im schlimmsten Fall existenzbedrohend sein kann", warnt Neusiedler.

Vier von zehn Österreichern
Im starken Gegensatz zu den Schutzmaßnahmen stehen die persönlichen Erfahrungen der Befragten: Immerhin mehr als 40 % der Studienteilnehmer geben an, dass entweder sie selbst oder jemand aus ihrem engsten Umfeld bereits einer Form von Internetbetrug zum Opfer gefallen ist. Am häufigsten genannt wurden Phishing-Nachrichten sowie gefälschte Mails und Websites. Danach folgen Hacks, der Diebstahl von finanziellen Daten und Erpressung.

„Cyber-Schutzmaske"
Internetkriminalität ist das am stärksten wachsende Kriminalitätsfeld in Österreich, wie auch das Kuratorium für Verkehrssicherheit (KFV) bestätigt. Daher bietet auch die Helvetia seit dem Vorjahr eine „Cyber-Versicherung" für Privatkunden an. Das Produkt mit dem Namen „Helvetia Card Home Cyber" ist laut Helvetia als Zusatzbaustein zur Haushaltsversicherung buchbar. Enthalten sind Informations- und Service-Leistungen und in bestimmten Versicherungsfällen Kostenersatz. Auch gibt es dazu eine 24-Stunden-Hotline für die Beratung in Schadenfällen im Zusammenhang mit Cyberkriminalität wie etwa Virenbefall, Cybererpressung, unerlaubter Veröffentlichung von Fotos, unberechtigter Abmahnung bei „Free"-Downloads, Identitätsdiebstahl, E-Mail-Betrug und vielem mehr.

FORTSETZUNG VON SEITE 21

Darf Beratung etwas kosten?

Analysieren und planen
In seinem eigenen Unternehmen begann es mit einer Analysephase, unter anderem mit einer Markt- und Umfeldanalyse sowie einer Machbarkeits-Analyse, was das Personal und den Zeitaufwand betrifft. Zusammen mit den strategischen-, Kunden- und Mitarbeiter-Anforderungen ermöglichte dies ein Grobkonzept Dienstleistung.

Daran anschließend brauchte es Planung der Leistungen zum Kundennutzen, der Prozesse und Abläufe, der Ressourcen, des Marketingkonzepts in der Beratung, der Argumentation sowie der Umsetzung mit Zeitplan.

Zwei Modelle
Daraus entwickelte Wienerroither ein „Produktmodell Dienstleistung", das beschreibt, „was geleistet wird, nicht wie"; plus ein Prozessmodell, das beschreibt, „wie die Ergebnisse einer Dienstleistung zustande kommen". Und intern brauche es ein „Ressourcenkonzept" zur Planung der Kapazitäten für die Erbringung der Dienstleistung: Wie viele Kunden können mit wie vielen Mitarbeiten und welchen verfügbaren Dienstleitungsstunden betreut werden?

Servicevertrag
Am Ende stand die interne Implementierung, die Bekanntmachung im Kundenstamm und am Markt und ein „Servicevertrag": mit klarer Regelung durch (neben den Allgemeinen Geschäftsbedingungen der Kanzlei) Geschäftsbedingungen hinsichtlich Vertragsdauer, Leistungen des Servicevertrages, Kündigungsmöglichkeiten, Kosten- und Inkassoregelung.

Erfolgskontrolle über die Servicevertrags-Regelung in der Praxis ergibt sich durch die Kundenzufriedenheit, die Mitarbeiterzufriedenheit und die Wirtschaftlichkeits-Betrachtung.

Foto: Winterroither

Martin J. Wienerroither, der Obmann-Stellvertreter der Fachgruppe der Versicherungsmakler der Wirtschaftskammer Niederösterreich, bejaht die kostenpflichtige Kundenbetreuung

Mut haben
Wienerroithers Fazit: Honorarverrechnung festigt die persönliche Kundenbindung und -beziehung: Seine Kunden seien „bereit", für Sonderleistungen zu zahlen. Alle seriösen Makler, die bereit seien, für ihre Kunden das nötige „Mehr" zu leisten bzw. sich von „Produktverkäufern" abheben wollen, sollten diese Leistungen nicht kostenlos erbringen. Daher lautet sein Appell: „Wer den Mut hatte, sich als Versicherungsmakler selbstständig zu machen, kann auch den Mut haben, für seine vielfältigen Leistungen zu Gunsten seiner Kunden Geld zu verlangen."