DSGVO-Tipp: Nützliche Leitfäden für die Praxis.

Machen Sie Ihr Unternehmen IT-sicher und schulen Sie Ihre Mitarbeitenden.

Auch die FMA hat 2019 den Prüfungsschwerpunkt Cyber Security.

Ziel ist: Gefahren zu erkennen, Sicherheitsstrategien zu entwickeln, Schutzmaßnahmen zu erarbeiten und täglich umzusetzen. Dazu haben wir nützliche Leitfäden für Sie zusammengetragen.

Im Vorjahr waren alle mit der Umsetzung der DSGVO intensiv beschäftigt. Ein Punkt dabei war, die technischen und organisatorischen Rahmenbedingungen des Unternehmens auch dahingehend zu überprüfen, ob ausreichend Sicherheit besteht. Sowohl für die eigenen Daten, als auch die personenbezogenen Daten der Kunden, Mitarbeiter, Partner usw.

Seither sind nun einige Monate vergangen. Zeit also, um sich wieder mit dem Thema zu beschäftigen. Denn einerseits liest man beinahe wöchentlich von einem Datendiebstahl, bei dem Millionen von kundenbezogenen Daten im Netz auftauchen. Andererseits legt Ihnen die **DSGVO die Verpflichtung auf, die Daten zu schützen, die Mitarbeiter zu schulen** bzw. zu überprüfen, ob man sich nach wie vor an die Vorgaben hält oder vielleicht doch wieder ein Schlendrian Einzug gehalten hat. Und womöglich hat sich in den letzten Monaten auch hinsichtlich der **Technik-Ausstattung im Haus etwas geändert**, was sich aber noch nicht in den DSGVO-Unterlagen niedergeschlagen hat. Zur Erinnerung: Dank DSGVO muss man ein Verarbeitungsverzeichnis erstellen, TOMs definieren und diverse Formalitäten erfüllen, die nun möglicherweise aktualisiert werden sollten.

Aktualität bekommt das Thema auch dadurch, dass die **FMA heuer einen Prüfschwerpunkt auf Cyber Security legen wird.** Daher erinnern wir an die FMA-Richtlinien, die sich mit Vorgaben zur IT-Sicherheit beschäftigen.

Wir möchten Sie aber nicht nur an Ihre Aufgaben erinnern, sondern auch auf **Hilfestellungen zu diesen Punkten hinweisen.**
Denn Datensicherheit ist nicht nur eine mühselige Aufgabe, die aufgrund der DSGVO entsteht, sondern auch eine Voraussetzung dafür, dass Sie Ihre Geschäfte langfristig betreiben können (bei Hackerangriff droht Daten- und womöglich auch Vertrauensverlust bei Ihren Kunden und Partnern).

Während sich in Großbetrieben und Konzernen mehrere Mitarbeiter um dieses Thema kümmern, lastet diese Aufgabe bei EPUs und KMUs meist auf einer Person, die noch dazu gleichzeitig viele andere Aufgaben zu erfüllen hat.

Gut ist, dass man vieles nicht neu erfinden muss, denn es gibt zahlreiche nützliche Checklisten und Leitfäden, auf die man zurückgreifen kann. Einige davon haben wir für Sie gesammelt und in diesem Beitrag zusammengestellt.

A) FMA-Leitfäden zur IT-Sicherheit

Wie oben erwähnt, wird die **FMA bei Prüfungen im Jahr 2019 einen Schwerpunkt** auf die Einhaltung der IT-Sicherheit legen.

Dazu wurde im Vorfeld eine Reihe von Leitfäden (für jede Branche) erstellt. Die Links dazu finden Sie am Ende des Beitrags.

In diesen Leitfäden weist die FMA darauf hin, dass auch im Finanz- und Versicherungsbereich **durch die Digitalisierung besonders die IT-Systeme** und die Gestaltung der digitalen Angebote zunehmend an Bedeutung gewinnen. Damit wachsen auch die **Risiken:** „Die Risiken eines Ausfalls von Systemen oder Missbrauchs von Daten können dabei sowohl die Unternehmen als auch die Versicherten treffen und im Extremfall sogar Stabilität und Vertrauen in den Finanzmarkt schädigen."

Und die FMA weiter: „Die zunehmende Digitalisierung des Versicherungsgeschäfts muss daher mit hohen Anforderungen an die Sicherheit der Systeme und Daten einhergehen. Wir wollen mit diesem Leitfaden auch das Vertrauen der Versicherungskunden in digitale Technologien und in die Datensicherheit erhöhen".

Und auch für den Finanzdienstleistungsbereich hat die FMA Leitfäden herausgegeben und weist dort darauf hin, dass die **Unternehmer auch für ihre Vermittler verantwortlich** sind.

„Die Leitlinien stellen überdies klar, dass Wertpapierdienstleister, die mit vertraglich gebundenen Vermittlern (VGV) oder Wertpapiervermittlern (WPV) zusammenarbeiten, dafür Sorge zu tragen haben, dass diesen zur Verfügung gestellte Kundendaten ausreichend geschützt werden."

Diese Leitfäden stellen eine **„Erwartungshaltung der FMA in puncto IT-Sicherheit klar**", d.h. sie sind keine gesetzlichen Vorschriften, aber die FMA weist klar darauf hin, dass sie die Einhaltung genau prüfen wird:

„Entsprechend den Aufsichts- und Prüfungsschwerpunkten der FMA für das Jahr 2018 dient der Leitfaden auch als Orientierungshilfe"

Gründe genug, sich die Leitfäden näher anzusehen und zu überlegen, was davon man vielleicht auch im eigenen Unternehmen berücksichtigen könnte:

https://www.fma.gv.at/fma-veroeffentlicht-leitfaden-zur-it-sicherheit-in-versicherungs-und-rueckversicherungsunternehmen/

https://www.fma.gv.at/fma-veroeffentlicht-leitfaeden-zur-it-sicherheit-bei-fonds-verwaltern-und-wertpapierdienstleistern/

https://www.fma.gv.at/fma-veroeffentlicht-leitfaden-fuer-die-digitale-sicherheit-in-banken/

https://www.fma.gv.at/fma-veroeffentlicht-leitfaden-it-sicherheit-fuer-pensionskassen/

https://www.fma.gv.at/fma/fma-leitfaeden/

B) Nützliche Leitfäden – vor allem für EPUs und KMUs – zum Thema IT-Sicherheit und TOMs im Rahmen der DSGVO

Unter dem Titel **„it-safe 2020"** hat das damalige Wirtschaftsministerium – heißt nunmehr Bundesministerium für Digitalisierung und Wirtschaftsstandort – gemeinsam mit der Wirtschaftskammer Österreich (WKO) **Ratgeber gezielt für KMUs und Ein-Personen-Unternehmen** erstellt, um diese Unternehmen darin zu schulen, Cyberbedrohungen besser erkennen und vermeiden zu können.

Denn **auch kleine Unternehmen müssen** „angemessene Datenschutzmaßnahmen nach dem Stand der Technik" aufgrund der DSGVO vorsehen. **Angemessen bedeutet,** dass man nicht die gleichen Anforderungen erfüllen muss, wie man das von einem Großunternehmen verlangen kann. Da aber auch bei Klein-Unternehmen Datenschutz und Datensicherheit immer stärker in den Fokus rücken, soll der folgende Leitfaden eine **Übersicht geben, welche technischen Sicherheitsvorkehrungen notwendig und sinnvoll sind** und wie Sie diese im Unternehmen umsetzen können.

a) IT-Sicherheits-Checkliste

Einen sehr guten Einstieg in das Thema bietet die IT-Sicherheits-Checkliste.
Hier werden grundlegende Informationen sehr benutzerfreundlich aufbereitet und Problembewusstsein geschaffen. Auch im Hinblick auf die DSGVO-Umsetzung. Das **PDF können Sie hier herunterladen…**

b) Leitfaden Sicherheitsmaßnahmen DSGVO

Bereits umfangreicher und möglicherweise **praxisrelevanter** für EPUs und KMUs ist der Leitfaden „Sicherheitsmaßnahmen DSGVO", den man sich ebenfalls als PDF herunter laden kann. Und zwar hier…

In diesem Leitfaden bekommt man zunächst einen **Überblick über grundlegende Faktoren** wie Firewall, Verschlüsselung, Cloud-Nutzung, Nutzung von VPN etc.

Dann bekommt man einen guten Überblick über die **Pflichten des Verantwortlichen basierend auf der DSGVO** (Verarbeitungsverzeichnis für Verantwortliche und Verarbeiter, TOMs, also die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten).

Danach folgt das **Kapitel „Mitarbeiter"**. IT-Sicherheit und Datenschutz können auch mit bester technischer Ausstattung nur dann funktionieren, wenn die Mitarbeiter „ausgeprägtes Sicherheitsbewusstsein besitzen und in der Lage sind, die Vorgaben in der täglichen Praxis umzusetzen". Daher sind **Schulung und Sensibilisierung wichtige Aufgaben!** Damit die Mitarbeiter verdächtige E-Mails erkennen können, damit sie bei Außerhaus-Arbeit (etwa vom Heimarbeitsplatz, im WLAN des Cafés etc.) kein ungeschütztes WLAN nützen, etc. Ein anderer wichtiger Punkt sind auch Personalwechsel, denn auch die neuen Mitarbeiter gehören geschult etc.

DSGVO-relevante Themen wie WLAN-Nutzung, Nutzung eigener Betriebsmittel (Handy, Laptop etc.), Nutzung von Social Media etc. werden ebenfalls behandelt.

Und dann folgen **drei Muster-Beispiele,** wie man sinnvollerweise in einem Unternehmen die technischen und organisatorischen Maßnahmen umsetzen könnte. Und zwar bei einem EPU, bei einem KMU mit 5 Mitarbeitern und einem KMU mit 20 Mitarbeitern. Entsprechend der Verhältnismäßigkeit steigen die Anforderungen hinsichtlich IT-Sicherheit und Datenschutz mit zunehmender Unternehmensgröße. Hier nochmals der Link zum **Herunterladen dieses Leitfadens…**

c) Mitarbeiter-Handbuch für IT-Sicherheit

Grundlegende Fakten zur IT-Sicherheit und EDV-/Internet-Nutzung erfährt man in einem Leitfaden, den man für **die Schulung der Mitarbeiter** nutzen kann, um diese für die Gefahren zu sensibilisieren, was möglicherweise hilft, **dass diese** nicht **in typische Internet-Fallen** tappen. Womit man Datendiebstahl und Hackerangriffe verhindert.

Es werden darin **wichtige Informationen gut verständlich aufbereitet.** Daher nicht nur für die Mitarbeiter nützlich, sondern auch für so manchen Chef.
Etwa: Der sichere Umgang mit personenbezogenen Daten. Die richtige Entsorgung von Papierdokumenten/Datenträgern. Sicherer Umgang mit mobilen IT-Geräten. Wirksame Passwörter. Spams und Phishing-Mails. Schadsoftware und Maßnahmen dagegen.

Dieses **PDF kann man hier herunterladen…**

Quelle: Homepage it-safe.at, WKO-Seite zu Innovation, Technologie/Digitalisierung