Leitfaden DSGVO – Thema: Technisch-organisatorische Maßnahmen

Die Technisch-Organisatorischen Maßnahmen (TOM) beschreiben, wie in einem Unternehmen die Sicherheit der Daten gewährleistet ist. Sie sind Grundlage für das Sicherheitsniveau beim Beschreiben Ihrer Verarbeitungstätigkeiten und Thema des dritten Teils des DSGVO-Leitfadens für eine gute Compliance-Strategie.

Integrität und Vertraulichkeit

Der Unternehmer hat Schutzmaßnahmen zu treffen, damit die personenbezogenen Daten seines Kunden nicht verloren gehen oder unbefugten Dritten in die Hände fallen.

Dafür ist es ausreichend, dass ein „angemessenes“ Schutzniveau eingerichtet wird, welches an den Risiken im Falle des Datenschutzverstoßes festzumachen ist. Damit wird dem DSGVO-Grundsatz der „Integrität und Vertraulichkeit“ (vgl. Art. 5 Abs. 1 Buchst. f DSGVO) entsprochen.

Angemessenes Schutzniveau

Sebastian Karch, Rechtsanwalt / Gesellschaftsrecht, Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft

Mit „angemessenes Schutzniveau“ hat man es allerdings wieder mit einem sogenannten unbestimmten Rechtsbegriff zu tun, der interpretationsfähig ist. Auch an dieser Stelle wird aber an den gesunden Menschenverstand appelliert: Wer beispielsweise sensible Kundendaten über WhatsApp versendet, hat offensichtlich keine Schutzmaßnahme getroffen. Deswegen muss sich jeder immer die Frage, ob die Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit der Datenverarbeitung beim einzelnen Verarbeitungsvorgang durch entsprechende Schutzmaßnahmen beachtet wird. Es gilt für jeden einzelnen Verarbeitungsvorgang zu prüfen, ob dazu eine „angemessene“ TOM getroffen wurde.

Verschlüsselung der Kommunikation

Die Verschlüsselung ist neben der Pseudonymisierung, die für Versicherungsmakler eher keine Option ist, eine gute Schutzmaßnahme. Dem Kunden sollte immer die Wahl gelassen werden, ob er die verschlüsselte Kommunikation wünscht oder in die unverschlüsselte Kommunikation einwilligt.

„Stand der Technik“

Überdies soll gewährleistet werden, dass die Daten auch nach eventuellen Zwischenfällen wieder rasch verfügbar sind. Dies Alles soll stets auf dem aktuellen Stand der

Technik erfolgen. Was unter „Stand der Technik“ genau zu verstehen sein soll, ist zwar nicht klar definiert, aber so zu verstehen, dass keine stark veraltete Software oder Software mit bekannten Sicherheitslücken verwendet werden soll. Tagesaktuelle Software hingegen muss nicht vorgehalten werden. Es gilt auch hier das sogenannte „Augenmaßprinzip“ von Behördenseite einzuhalten.

Diese Begrifflichkeit ist im Blick zu halten, um eventuelle Verschärfungen bei der Auslegung zeitnah mitzubekommen. Informationen gibt es zum Beispiel beim Bundesministerium des Inneren (BSI), welches zu den Mindeststandards für den Einsatz von Verschlüsselungsprotokollen regelmäßig Veröffentlichungen publiziert.

https://www.experten.de/2018/09/03/dsgvo-leitfaden-thema-der-datenschutzbeauftragte/

https://www.experten.de/2018/09/06/dsgvo-leitfaden-thema-verzeichnis-und-datenschutz-folgenabschaetzung/

Bilder: (1) © denisismagilov / fotolia.com (2) © Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4945370/leitfaden-dsgvo-thema-technisch-organisatorische-massnahmen/