Im Mai dieses Jahres jährt sich das Inkrafttreten der DSGVO schon zum zweiten Mal. Doch weiterhin werden Anpassungen vorgenommen, Neuerungen beschlossen und lange Geplantes wird angegangen. Es gilt daher, sich stets auf dem Laufenden zu halten und sich für den Umgang mit personenbezogenen Daten zu sensibilisieren.

ANGEMESSENE VORBEREITUNG HILFT DATENSCHUTZVERGEHEN ZU VERMEIDEN:

DIE DSGVO UND IHRE FOLGEN

Seit dem Inkrafttreten der Datenschutz-Grundverordnung, kurz DSGVO, am 25. Mai 2018 justierte die Bundesregierung das Gesetz wiederholt nach, weitere Anpassungen sind geplant. Für Unternehmen und Behörden bedeutet dies, dass der Datenschutz weiter im Fokus bleibt – und zwar auf verschiedenen Ebenen. Zum Datenschutz gehören nämlich nicht nur der datenschutzkonforme Umgang mit sensiblen Daten, sondern auch die richtige Handhabung von Websites, sicheren Passwörtern oder Diensthandys und -laptops. Erfolgt nämlich eine Nichtbeachtung des Datenschutzes, können Sanktionen und hohe Bußgelder die Folge sein.

Dokumentationspflichten beachten

Die technischen Entwicklungen nehmen rapide zu, die damit verbundene Menge an digitalen Daten und Datentransfers ist inzwischen gigantisch und aus dem alltäglichen Leben und der Arbeitswelt nicht mehr wegzudenken. Damit einhergehend entstehen die Dokumentations- und Nachweispflichten. Zu den Dokumentationspflichten zählen die Auftragsverarbeitung, die explizite Pflicht, alle Datenschutzverletzungen zu melden, sowie die Dokumentation von Abwägung und Garantie bei der Datenübermittlung an Drittländer, also Staaten außerhalb Deutschlands, der EU und des Europäischen Wirtschaftsraums, zu erstellen.

Bei der Auftragsverarbeitung handelt es sich um einen Prozess, bei dem Unternehmen als Auftraggeber personenbezogene Daten an Dritte, bspw. externe Dienstleister wie Druckereien, weitergeben, damit diese die Daten verarbeiten können oder andere, z. B. IT-Systemhäuser, Zugriff auf sie bekommen. Der Auftraggeber muss sicherstellen, dass der Datenschutz durch die Auftragnehmer gewährleistet ist, und einen Vertrag zur Auftragsverarbeitung schließen.

Nachweispflichten nachkommen

Es gilt außerdem, die Einhaltung der Verarbeitungsprinzipien, z. B. durch ein Datenschutzkonzept, nachzuweisen. Es muss ein Nachweis über die Einhaltung der DSGVO für besonders schützenswerte Daten wie bspw. Gesundheitsdaten erbracht werden. Zu den Pflichten gehört auch die Datenschutz-Folgeabschätzung, bei der es sich im Grunde um eine erweiterte Vorabkontrolle handelt, die schon im alten Bundesdatenschutzgesetz gefordert war. Sie ist immer dann notwendig, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, es sich um die weiträumige Überwachung öffentlicher Bereiche handelt, es um die Verarbeitung von Daten besonderer Kategorien oder Daten über strafrechtliche Verurteilungen und Straftaten geht.

Umgang mit Diensthandys und -laptops

Im Berufsalltag selbst gilt es, auf die Umsetzung der DSGVO zu achten. Laute Telefonate über sensible Firmendaten in der Öffentlichkeit gilt es möglichst zu vermeiden und bei der Nutzung von Dienstlaptops unterwegs Blickschutzfilter zu verwenden. Ebenso sollten Mitarbeiter keine öffentlichen WLANs nutzen, da diese in den meisten Fällen als nicht sicher gelten. Virtuelle private Netzwerke, sogenannte VPNs, bieten Alternativen. Zudem sollten Mitarbeiter ihre Passwörter regelmäßig ändern – ein sicheres Kennwort besteht aus acht bis zwölf Zeichen in Groß- und Kleinschreibung und enthält sowohl Buchstaben als auch Ziffern und Sonderzeichen. Gleiches gilt auch für den Schutz von Diensthandys, die sich ebenfalls mithilfe eines Passworts statt einer kurzen Zahlenkombination oder eines einfachen Wischmusters schützen lassen.

Bei der Nutzung von Diensthandys sind auch Messengerdienste problematisch. Die deutschen Aufsichtsbehörden für Datenschutz erachten viele von ihnen, darunter WhatsApp, als nicht datenschutzkonform. Manche Dienste haben nicht nur Zugriff auf alle in einem Smartphone gespeicherten Telefonnummern und Kontaktdetails, sondern übermitteln sie zusätzlich in Drittländer. Wer auf Kurznachrichten nicht verzichten möchte, kann auf andere datenschutzkonforme Apps zurückgreifen oder SMS versenden.

Datenschutzkonforme Unternehmenswebsites

Auch Unternehmenswebsites müssen den aktuellen Bestimmungen entsprechen. Um eine Website gesetzeskonform zu gestalten, reicht es nicht aus, eine allgemeine Datenschutzerklärung irgendwo zu kopieren oder automatisiert generieren zu lassen und dann zu veröffentlichen. Jede Website besitzt nämlich eine individuelle Struktur und verwendet unterschiedliche Plug-ins oder Cookies. Da den Aufsichtsbehörden zufolge bereits IP-Adressen als personenbezogene Daten gelten, benötigt jede Website, die diese speichert, eine Datenschutzerklärung. Mit deren Veröffentlichung auf der Website kommen Betreiber ihrer Informationspflicht nach – aber nur bei korrekter Formulierung. Nutzer müssen anhand dieser Erklärung nachvollziehen können, welche ihrer personenbezogenen Daten verarbeitet werden, und es gilt, sie in „klarer und einfacher Sprache" zu verfassen und darüber hinaus noch in „präziser, transparenter, verständlicher und leicht zugänglicher Form" zur Verfügung zu stellen.

Zudem darf die Datenschutzerklärung kein Bestandteil des Impressums sein, wenn hier keine eindeutige Kennzeichnung erfolgt. Darüber hinaus muss die Erklärung Details der Betroffenenrechte umfassen. Dazu zählen u. a. das Beschwerderecht und das Recht auf Widerruf. Besteht die Absicht, die Daten in Drittstaaten zu übertragen, muss auch darüber eine Aufklärung erfolgen. Seit Oktober 2019 ist auch der Einsatz von Cookies nur dann erlaubt, wenn sie für den technischen Betrieb von Websites erforderlich sind. Alle anderen Cookies benötigen eine Einwilligung des Nutzers. Diese Einwilligung muss aufgrund einer eindeutigen, aktiven Handlung der betreffenden Person erfolgen. Darüber hinaus ist es notwendig, über Datenverarbeitung und Speicherdauer zu informieren. Außerdem muss der Nutzer jederzeit die Möglichkeit haben, die Einwilligung zu widerrufen.

Mögliche Bußgelder

Halten Unternehmen diese Vorgaben nicht ein, können Sanktionen folgen. Diese sollen grundsätzlich bewirken, dass sich Unternehmen an die DSGVO halten und sich mit ihr auseinandersetzen. Oft erfolgen zunächst Mahnungen und eventuell verhängte Strafen müssen verhältnismäßig sein – nach Artikel 83 der DSGVO sind diesbezüglich bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweit erzielten Jahresumsatzes möglich. Sanktionen und die Höhe der Strafgelder richten sich nach der Art der Verstöße. Es spielt z. B. eine Rolle, wie viele Personen die Datenschutzverletzung betrifft, ob das Unternehmen absichtlich handelte oder ob sich die Firma kooperativ verhält. Erhalten Unternehmen eine Anfrage ihrer Datenschutzbehörde, sollten sie den Beistand eines Experten ersuchen.

Meist beginnt eine Untersuchung damit, dass Unternehmen einen mehrseitigen Fragebogen zugesendet bekommen, den die Mitarbeiter häufig eher arglos ausfüllen – sie kopieren z. B. die entsprechenden Antworten und Daten aus dem Internet. Eine solch unbedachte Vorgehensweise fällt den Aufsichtsbehörden sofort auf und kann im Zweifelsfall kostspielige Folgen für Unternehmen haben. Außerdem lassen sich Datenschutzverletzungen durch einfache Maßnahmen, bei denen Experten helfen können, vermeiden, sodass auch dem ordnungsgemäßen Austausch mit den Behörden nichts im Wege steht. <<

Visitenkarte

in

Haye Hösel

Zertifizierter Datenschutzbeauftragter, Inhaber und Gründer der HUBIT Datenschutz GmbH & Co. KG

E-Mail: info@hubit.de
Telefon: +49 421 331 14 300