SCHADEN.NEWS

12.08.2020

„DATENSCHUTZ IST CHEFSACHE“

Der Datenschutz gehörte in der breiten Öffentlichkeit, zumindest bis zum Wirksamwerden der DSGVO am 25.05.2018, nicht gerade zu den prioritären Themen. Allerdings war die DSGVO bereits am 24.05.2016 in Kraft getreten, so dass genügend Zeit zur Vorbereitung bestanden hätte. Da sie aber weitgehend ignoriert wurde, traf das Wirksamwerden viele so unverhofft wie Weihnachten und schlug ein wie die sprichwörtliche Bombe. Die Folge waren Hektik, Aufregung und Aufwand.

WORIN BESTANDEN (UND BESTEHEN) DIE HERAUSFORDERUNGEN?

Das Ausmaß der mit dem Datenschutz verbundenen Herausforderungen hing und hängt maßgeblich von der Sorgfalt ab, die dem Thema gewidmet wurde und wird. Wer schon vor der DSGVO auf eine strukturierte und abgesicherte IT sowie auf den sorgfältigen Umgang mit Kunden- und Mitarbeiterdaten Wert gelegt hatte, den brachte auch die DSGVO nicht aus der Ruhe. Wer das Thema hingegen vernachlässigt hatte, musste sich plötzlich mit der Inventarisierung seiner EDV, der Überprüfung der TOMs (Technische und organisatorische Maßnahmen), der Erstellung von Verzeichnissen der Verarbeitungstätigkeiten (Art. 30 DSGVO) oder Ablaufplänen für den Fall einer Datenpanne auseinandersetzen. Die Durchführung einer Risikoanalyse und Folgenabschätzung (Art. 35 DSGVO) sowie ggf. die anschließende Absicherung von Netzwerken oder die datenschutzkonforme Aus- und Umgestaltung von Arbeitsplätzen zählten ebenso dazu, wie die (wiederkehrende) Schulung der Mitarbeiter.

Grundsätzlich gilt, „Datenschutz ist Chefsache“ – und dieser sollte sich, soweit vorhanden, mit dem für den Betrieb zuständigen Datenschutzbeauftragten oder anderen Experten abstimmen (siehe dazu auch Infobox links).

INTERNER ODER EXTERNER DATENSCHUTZBEAUFTRAGTER?

Wenn in einem Betrieb mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist die Bestellung des Datenschutzbeauftragten obligatorisch. Einzelfallabhängig kann ein Datenschutzbeauftragter aber auch darunter sinnvoll sein. Ob dieser intern oder extern beschäftigt wird, muss jeder Betrieb für sich selbst entscheiden. Der Kündigungsschutz des internen Datenschutzbeauftragten kann dabei ebenso eine Rolle spielen, wie das Erfordernis zur ständigen Weiterbildung, die Nähe zum Unternehmen oder der Erfahrungshorizont. Insbesondere bei kleineren Unternehmen kann es vorteilhaft sein, wenn der Datenschutzbeauftragte über ein „weiteres Sichtfeld und Routine“ verfügt, wenn es um den Umgang mit den Datenschutzbehörden, z.B. bei der Meldung von Verstößen geht.

Abgesehen davon ist datenschutzrechtliche Konformität keine einmalige Maßnahme, sondern ein ständiger Prozess. Die Sicherstellung des jeweils aktuellen Stands der Technik macht daher Rückstellungen für und Investitionen in Hard- und Software ebenso unumgänglich, wie die fortlaufende Aktualisierung des Wissens.

DIE VERNACHLÄSSIGUNG DES DATENSCHUTZES KANN TEUER WERDEN!

Die ausgebliebene Abmahnwelle und die – von Ausnahmen abgesehen – durchaus als moderat zu bezeichnende Höhe der verhängten Bußgelder kann – bei oberflächlicher Betrachtung – den Eindruck erwecken, dass sich auch unter der DSGVO eigentlich verändert hat. Wer aber bereits der Attacke abmahnwütiger Verbraucher, die meinen in der DSGVO eine neue Verdienstmöglichkeit gefunden zu haben, ausgesetzt war oder ein Schreiben der Landesdatenschutzbehörde erhalten hat, weil die Cookie-Erklärung auf der Webseite nicht datenschutzrechtskonform war, weiß, dass dem nicht so ist.

Zudem kann derjenige, der z.B. schon einmal E-Mails mit offenem Verteiler verschickt oder den „falschen“ Kunden angeschrieben hat, ein Lied davon singen, wenn Betroffene plötzlich nicht nur Auskunft über ihre Daten, sondern auch überzogene Schmerzensgelder verlangen. Selbst wenn die Behörde angesichts zunehmenden Querulantentums nichts weiter unternehmen sollte, ändert dies nichts an dem Aufwand, der mit einer Meldung bzw. Stellungnahme verbunden ist. Anderseits zeigt sich gerade bei solchen Anlässen, ob und wie gut die Umsetzung der datenschutzrechtlichen Anforderungen funktioniert hat.

WELCHE BUSSGELDER WURDEN BISHER VERHÄNGT?

Die Höhe der Bußgelder ist in Europa uneinheitlich. Gemäß Art. 83 Abs. 1 DSGVO sollten Bußgelder „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein.

Die Spanne der in Deutschland im Millionenbereich verhängten Bußgelder liegt zwischen 1,24 Mio. Euro (AOK Baden-Württemberg) und 14,5 Mio. Euro (Deutsche Wohnen). Das von der britischen Datenschutzbehörde gegenüber der Decision Technologies Limited – die über 16 Millionen Werbe-E-Mails auf Basis einer unwirksamen Einwilligungserklärung verschickt hatte – verhängte Bußgeld in Höhe von 99.524 Euro, wirkt dagegen nahezu wie ein Trinkgeld. Wie sich die Bußgelder in Deutschland berechnen, darüber berichtete schaden.news im Februar dieses Jahres.

Dennoch zeigt der Fall der AOK, bei dem über einen längeren Zeitraum die Daten von 500 Versicherten für Gewinnspiele verwendete wurden, ohne dass hierfür eine Einwilligung vorlag, wie wichtig es ist, dass datenschutzrechtliche Konzepte nicht nur auf dem Papier , sondern sich auch in den Prozessen an sich vorhanden sind.

WAS GILT FÜR SOCIAL MEDIA UND DEN PRIVACY-SHIELD?

Mit der Aussage „DSGVO und Social Media passen nicht zusammen“ ist es wie mit allen Pauschalbehauptungen: Sie können passen, müssen aber nicht. Was z.B. Whatsapp angeht, so können die Nutzer sicher sein, dass ihre und die Daten der Kontakte an Whatsapp - und möglicherweise auch an andere Unternehmen in den USA - übermittelt und dort ausgelesen werden, ohne dass sich dies unterbinden lässt. Wer Whatsapp und nicht eine der vorhandenen unbedenklichen Alternativen nutzen möchte, sollte dies aus den genannten Gründen tunlichst nicht über das Firmenhandy tun.

Bei der Einbindung von Social-Media in den Webauftritt ist unbedingt darauf zu achten, dass sich diese in der Datenschutzerklärung wiederfinden. Wie es mit den USA-gestützten-Social-Media rechtlich weitergeht, ist nach dem Ende des Privacy Shield aktuell schwer vorhersagbar, auch wenn die Standard-Vertragsklauseln derzeit noch einen Ausweg bieten. Wer seine Daten bei einem US-basierten Dienstleister speichert, sollte sich indes zusichern lassen, dass die Verarbeitung ausschließlich in der Europäischen Union erfolgt. Wo dies nicht möglich ist, sollte ggf. ein Wechsel des Dienstleisters erwogen werden.

ZUSAMMENFASSUNG

Man mag zu der DSGVO stehen, wie man will. Als Betriebsinhaber – gleich ob mit drei oder mehr als 50 Angestellten – kommt man nicht umhin, sich mit diesem Thema zu beschäftigen. Wer den Datenschutz aus Mangel an Zeit – oder auch Interesse – bisher von sich weggeschoben hat, dem sei gesagt: Es ist ein gefährliches Glücksspiel. Den die drohenden Bußgelder bei einem gemeldeten Verstoß oder einer unvorhergesehenen Überprüfung durch die Behörden können „schmerzhaft“ wenn nicht gar existenzbedrohend sein.

Dr. Wolf-Henning Hammer (ETL Kanzlei Voigt)