IN DIESER AUSGABE:

Newsletter Oktober 2019

Datenschutz

Liebe Leserinnen und Leser,
die vielen Entscheidungen und Fragestellungen im Zusammenhang mit der DS-GVO zeigen, dass gesetzeskonformer Datenschutz nicht einfach mal so umgesetzt werden kann und zudem auch noch nicht alle Themen 100 Prozent konkretisiert sind. Fakt ist, dass die Bedeutung des Datenschutzes immer größer wird. Hier ein paar Auszüge aus den News der letzten drei Monate.

ISO 27701 – Eine Zertifizierung für den Datenschutz?

In der DS-GVO wird eine Zertifizierung des Datenschutzes deutlich gefordert. Mit der ISO 27701 ist nun erstmalig eine Norm zum Nachweis der datenschutzrechtlichen Vorschriften veröffentlicht worden. Diese neue Norm ist eine Erweiterung der ISO 27001, die das Thema „Informationssicherheit“ behandelt. Ist ein Unternehmen also ISO 27001 zertifiziert, kann es mit relativ wenig Aufwand, auch den Nachweis für einen geprüften Datenschutz erbringen. Viele Maßnahmen der ISO 27001 sichern ohnehin den Schutz der personenbezogenen Daten und die Schutzziele „Vertraulichkeit, Integrität und Verfügbarkeit“ sind zudem identisch. Hier wird deutlich, wie eng die Themen Informationssicherheit und Datenschutz miteinander verbunden sind. Einen Haken hat die neue ISO 27701 jedoch: Die DSGVO fordert eine zertifizierbare Ausrichtung auf Produkte und Prozesse, bei der ISO 27001 stehen hingegen Managementsysteme im Vordergrund. Das bedeutet, dass eine Zertifizierung der Datenschutzkonformität über die ISO 27001 nur indirekt erreicht werden kann. Denkbar wäre dies jedoch durch Hinzufügung der Anforderungen der ISO 27701 im Statement of Applicability (SOA) des ISO 27001-Zertifikats. Unseres Erachtens ist die Integration der ISO 27701 eine richtige und pragmatische Lösung zum Nachweis datenschutzkonformen Handelns innerhalb des betriebenen ISMS.

Cookies setzen – aber wie?

Der Europäische Gerichtshof (EuGH) hat entschieden, dass Cookies, die nicht unbedingt erforderlich sind, nur nach einer aktiven Einwilligung gesetzt werden dürfen. Was bedeutet dies für die Praxis? Entscheidend ist hier die Formulierung „aktiv“. Aktiv ist eine Einwilligung nur dann, wenn das Häkchen im Cookie-Banner selbständig gesetzt wird (Opt-In-Verfahren). Ein bereits vorausgefülltes Feld ist nach Ansicht des EuGH keine „Willensbekundung“ und demnach unwirksam. Hierbei ist es völlig unbedeutend, ob es sich bei den übermittelten Daten um personenbezogene oder nicht-personenbezogene Daten handelt. Einfache Cookie-Banner, die man wegklicken oder stehen lassen kann, reichen nach dieser Rechtsprechung nicht mehr aus. Erschwerend hat der EuGH zudem erklärt, dass Websitebetreiber gegenüber dem Nutzer auch Angaben zur Funktionsdauer und zu Zugriffsmöglichkeiten Dritter machen müssen. Hierzu sollte man aber die weitere Rechtsprechung abwarten. Zudem ist die praktische Umsetzbarkeit derzeit noch sehr begrenzt. Wichtig ist für Websitebetreiber im ersten Schritt die Wahl eines Cookie-Banners mit Opt-In-Verfahren.

Die Falle des „Gefällt-Mir-Buttons“

Die Tücke bei Social-Plugins ist, dass diese beim Öffnen einer Website sofort die IP-Adresse und damit alle mit ihr verbundenen Informationen an den Social-Media-Anbieter weiterleiten. Dies führte dazu, dass der EuGH entschieden hat, dass der Websitebetreiber gemeinsam mit dem Social-Media-Anbieter verantwortlich für die Erhebung und Übermittlung der personenbezogenen Daten ist. Für den Grad der Verantwortung kommt es allerdings auf die Umstände des Einzelfalles an, jedoch ist der Websitebetreiber nicht für die über die Erhebung und Übermittlung hinausgehende Datenspeicherung verantwortlich. Nach Meinung des EuGH besteht auch bei Social-Plugins eine Informationspflicht sowie die Pflicht zur Einholung einer Einwilligung. Websitebetreiber sollten daher beim Einbinden von „Gefällt-Mir-Buttons“ oder anderen Social-Plug-Ins unbedingt auf eine 2-Klick-Lösung zurückgreifen. Hierbei ist der Button standardmäßig deaktiviert und wird erst durch einen bzw. zwei Klicks aktiviert und somit die Empfehlung ausgesprochen. Die Shariff-Lösung von Heise ist hier beispielsweise eine gute Alternative.

Die „Macht“ der Datenschützer über Fanpages

Im Juni 2018 entschied der EuGH, dass die Betreiber einer Facebook-Fanpages für die Sammlung von Nutzerdaten, die durch Facebook im Hintergrund erfolgt, mitverantwortlich sind. Das die technische Infrastruktur vollständig von Facebook stammt ist hierbei nicht relevant. Die Reaktion von Facebook, eine Vereinbarung beim Erstellen einer Fanpage zu hinterlegen, reichte Datenschützern nicht aus. Anhand eines Präzedenzfalles hat das Bundesverwaltungsgericht in Leipzig im September 2019 entschieden, dass die Datenschutzaufsichts-behörden nun das Recht haben, Betreiber einer Facebook-Fanpage zu verpflichten, ihre Unternehmensseite abzuschalten, sofern schwerwiegenden datenschutzrechtlichen Mängeln festgestellt werden. Betreiber von Fanpages sind nach Ansicht der Aufsichtsbehörde in Kiel in der Pflicht, von Facebook die Datenschutzkonformität für die mit dem Betrieb dieser Fanpages verbundene Datenverarbeitung einzufordern. Da der Seitenbetreiber und Facebook eine gemeinsame Verantwortung für die jeweilige Fanpage tragen, kann nur auf diesem Wege nachgewiesen werden, dass der Seitenbetreiber alles in seiner Macht stehende getan hat, um mit seiner Fanpage den Datenschutzvorgaben gerecht geworden zu sein. Vor diesem Hintergrund empfehlen wir eine Überprüfung der betriebenen Facebook-Fanpage, um hohe Bußgelder und die zwangsweise Abschaltung der Fanpage zu verhindern.

Ein Modell zur Berechnung von Bußgeldern

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich auf ein neues Modell zur Berechnung von Bußgeldern verständigt, das im Ergebnis zu sehr hohen Sanktionen führen kann. Vereinfacht dargestellt, wird in diesem sehr komplexen Rechenmodell ein umsatzbasierter Tagessatz ermittelt, der mit Faktoren, die sich aus der Schwere des Verstoßes ergeben, multipliziert wird. Durch die Ausgangsschwere des Verstoßes sowie weitere erschwerende oder mildernde Umstände wird dieser Wert entsprechend korrigiert. Dieses Modell wird von vielen Fachleuten aber in Hinblick auf die in der DS-GVO geforderten Verhältnismäßigkeit durchaus kritisch betrachtet. Fakt ist jedoch, dass von einer Verschärfung des Themas Bußgeld ausgegangen werden muss.

Wenn Sie Fragen oder Interesse an weiteren Informationen zu den vorgestellten Themen haben, wenden Sie sich gern an Ihren Datenschutzbeauftragten der ANMATHO AG.