UIMCommunic@tion

06/2019

Ausgabe für Deutschland

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Datenschutzanpassungsgesetz bringt keine Erleichterung: Auch ohne Datenschutzbeauftragten muss Datenschutz eingehalten werden

Der Bundestag hat sich noch kurz vor der Sommerpause mit der Implementierung der Datenschutzgrundverordnung beschäftigt. Mit dem Zweiten Datenschutzanpassungsgesetz (2. DSAnpUG) wurde in vielen nationalen Gesetzen eine Anpassung auf die seit dem 25. Mai 2018 bereits unmittelbar gültige Datenschutzgrundverordnung vorgenommen. Betroffen sind von dem Paket insgesamt 154 einzelne Gesetze.

So beschloss der Bundestag die Schwelle, ab der Betriebe einen betrieblichen Datenschutzbeauftragten (DSB) ernennen müssen, von 10 auf 20 Mitarbeiter zu erhöhen. Auf den Punkt gebracht könnte man sagen: Die Pflichten bleiben gleich, aber zuständig ist niemand mehr. Denn tatsächlich gelten auch für die Betriebe, die jetzt von der Pflicht zur Bestellung eines DSB „befreit“ wurden, die gleichen datenschutzrechtlichen Vorgaben wie zuvor.

Neben der Änderung bei der Bestellung des Datenschutzbeauftragten entfällt die Schriftformerfordernis für die Einwilligung im Beschäftigtenverhältnis. So können Einverständniserklärungen künftig auch elektronisch erfolgen. Dies vereinfacht z. B. die Einwilligung für die Veröffentlichung von Fotos auf der Firmenwebsite, indem nur noch im Rahmen einer E-Mail mit angehängtem Foto um das Einverständnis gebeten werden muss. Natürlich müssen Aspekte wie Widerspruch, Zweck oder Ort der Veröffentlichung genannt werden, doch entfällt die „Zettelwirtschaft“. „Ganz nebenbei ist dies auch ein Argument für einen Datenschutzprofi im Hause: Wer informiert Sie denn sonst über solche Datenschutz-Erleichterungen?“ fragt Dr. Haaz mit einem Augenzwinkern. Noch sind die Änderungen nicht in Kraft. Da es sich um ein zustimmungspflichtiges Gesetz handelt, muss der Bundesrat ebenfalls positiv votieren. Der gesamten Text unter www.uimc.de/kommunikation/pressemitteilungen.

Marriott und British Airways drohen hohe Strafzahlungen

Die Datenschutzgrundverordnung ist ein gutes Jahr in Kraft. Ihre Wirkung wird immer sichtbarer und für einige Unternehmen spürbar – gerade was die Höhe von Strafen betrifft. In Großbritannien gibt es in dieser Woche zwei spektakuläre Fälle: Zunächst verhängte die Datenschutzbehörde Großbritanniens (ICO) gegen die Fluggesellschaft British Airways ein Bußgeld in Höhe von 205 Millionen Euro. Jetzt traf es die US-Hotelkette Marriott. Sie soll ein Strafgeld von 110 Millionen Euro entrichten. Was ist aus den zwei britischen Fällen zu lernen?

Bei einem Angriff hatten Cyberkriminelle 2018 persönliche Daten und Kreditkarteninformationen inklusive Sicherheitscodes (CVV-Nummern) von Kunden der Airline erbeutet. Betroffen waren Kunden der Fluggesellschaft, die auf der Website BA.com oder über die Mobil-App zwischen dem 21. August und dem 5. September eine Buchung vornahmen. Der Vorwurf der britischen Datenschutzbehörde Information Commissioner’s Office (ICO) ist eindeutig: Der Datenabgriff aus dem Sommer 2018 sei auf gravierende Sicherheitsmängel bei der Fluglinie zurückzuführen.

Genauso im Fall der US-Hotelkette Marriott. Das ICO hat eine geplante Strafzahlung von knapp 110 Mio. Euro angekündigt. Das Datenleck bei Marriott war Ende November bekannt geworden. Es hatte sich auf der vom Mitbewerber Starwood übernommenen Gästedatenbank befunden. Insgesamt waren nach Unternehmensangaben etwa 383 Mio. Datensätze betroffen, darunter Ausweis- und Kreditkartennummern. Es wird angenommen, dass die Systeme der Starwood-Hotelgruppe ab 2014 angegriffen wurden. Marriott erwarb Starwood im Jahr 2016, aber die Offenlegung von Kundeninformationen wurde erst 2018 entdeckt. Die Untersuchung des ICO ergab, dass Marriott beim Kauf von Starwood keine ausreichende Sorgfaltspflicht übernommen hat und auch mehr hätte tun sollen, um seine Systeme zu sichern. Der gesamten Text unter www.uimc.de/kommunikation/pressemitteilungen.

Update zum Info-Brief 05-2019: Transparenz der Rechtsgrundlage

Einzelne Aufsichtsbehörden haben hinsichtlich der BVerwG-Entscheidung zur Videoüberwachung mitgeteilt, dass vorerst nicht mit Verwarnung, Anweisung oder Geldbuße vorgegangen wird, sofern auf Hinweisschildern auch Art. 6 Abs. 1 Satz 1 lit. f DSGVO als Rechtsgrundlage genannt wird. Es wurde aber empfohlen, mittelfristig die Hinweisschilder zu überarbeiten und § 4 BDSG zu streichen. Innerhalb des Online-Formular-Centers finden Sie eine aktualisierte Version (www.online-formular-center.eu).

UIMC® | in Datenschutz und Informationssicherheit stets gut beraten!

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal

Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Rechtsgrundlage bei der Datenverarbeitung von personenbezogenen Daten eines Ansprechpartners (B2B-Geschäft)

Artikel 6 Abs. 1 lit. b DSGVO („die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen“) ist als Rechtsgrundlage nur dann einschlägig, wenn die Vertragsbeziehung zu der natürlichen Person selbst besteht, um deren Daten es geht (bspw. B2C/Verbraucher oder andere Einzelpersonen wie Selbständige).

Wenn die Vertragsbeziehung dagegen mit einem Unternehmen besteht (B2B), und es werden personenbezogene Daten von deren Mitarbeiter verarbeitet, wäre Artikel 6 Abs. 1 lit. f DSGVO die einschlägige Rechtsgrundlage („die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen[...]“, soweit und solange es für die Geschäftsbeziehung zu dem Unternehmen erforderlich ist.

Dies ist zum Beispiel im Rahmen der Informationspflichten gemäß Artikel 13/14 DSGVO transparent zu machen. Muster und Templates finden Sie unter www.Online-Formular-Center.eu.

News Informationssicherheit

Ransomware-Attacken oder mit Malware wie Emotet haben in den letzten Monaten zahlreiche Unternehmen getroffen und geschädigt. Cyber-Kriminelle nutzen hierbei gerne die weit verbreiteten Software-Produkte, um möglichst viele Systeme einfach zu infizieren, wie z. B. Microsoft Office. Hierbei sind beliebte Angriffswege die Makro-Funktion in Word oder aktive HTML-Anzeigen in Outlook.

Das BSI hat daher Empfehlungen für eine sichere Konfiguration der gängigen Microsoft-Office-Produkte erstellt. Damit können Sie die Angriffsfläche signifikant reduzieren: Die Deaktivierung von HTML in E-Mails sowie der sichere Umgang mit Makros in Dokumenten und anderen Dateien sind dabei nur zwei von zahlreichen Empfehlungen. Näheres finden Sie unter www.bsi.bund.de oder kommen Sie auf uns zu.

Neue Unterlagen im Online-Formular-Center

- Joint-Controller-Vertrag (Artikel 26 DSGVO) (neu)
- Informationspflichten für Videoüberwachung (aktualisiert)
- Merkblatt zum Datenschutzhandbuch (neu: Bereich „Einkauf“)

www.online-formular-center.eu

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

☐ Vorbeugende Maßnahmen, um Strafen zu verhindern

☐ Datenschutzkonforme Installation von Videokameras

☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 946 7726 9200 oder formlos per Mail an communication@uimc.de

Mehr Informationen, Hinweise und Tipps finden Sie hier: https://communication.UIMC.de