UIMCommunic@tion

06/2019

Ausgabe für Österreich

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Marriott und British Airways drohen hohe Strafzahlungen – DSGVO findet europaweite Anwendung

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. „Die zwei Fälle beweisen: Die DSGVO wird angewandt und für Unternehmen, die sie nicht beachten, richtig teuer", kommentiert der erfahrene Datenschutzfachmann Dr. Heiko Haaz die jüngsten Entwicklungen. Außerdem werde die DSGVO europaweit angewendet und nicht, wie von Kritikern oft eingewendet, nur in Deutschland oder Österreich. Was ist aus den zwei britischen Fällen zu lernen?

Ein Blick in die Einzelheiten der beiden Datenschutz-Fälle auf der Insel ist lohnenswert. Was war bei British Airways passiert und führte zur Androhung des hohen Bußgeldes von 205 Mio. Euro? 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. Persönliche Daten sind genau das – persönlich und deshalb müsse sich ein Unternehmen sorgfältig um diese Daten kümmern, so argumentiert die britische Datenschutzbehörde glasklar.

Sollte British Airways zahlen müssen, wäre es die höchste Strafe in der EU seit Einführung der DSGVO im Mai 2018. Das bisher höchste DSGVO-Bußgeld liegt bei 50 Millionen Euro und wurde von der französischen Datenschutzbehörde gegen Google verhängt. Allerdings: British Airways will Widerspruch gegen das 205-Millionen-Bußgeld einlegen. Trotzdem bleibt der Eindruck: Die DSGVO zeigt Zähne. Auch der Image-Schaden ist für BA sicherlich nicht zu unterschätzen.

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 Marriott-Fall zeigt, dass gerade bei der Übernahme eines Unternehmens eine hohe Sorgfaltspflicht besteht. Es sind Überprüfungen, Einschätzungen und Rechenschaftsmaßnahmen notwendig, um beurteilen zu können, welches Datenschutzniveau auch bei ‚eingekauften Datenverarbeitungssystemen' herrscht", betont Dr. Haaz, Partner der UIMC und mehrfach bestellter Datenschutzbeauftragter. Andernfalls könne eine Übernahme datenschutzrechtlich schnell eine teure Angelegenheit werden. Bei der Größenordnung nicht verwundernswert: Auch die Hotelgruppe Marriott, mit mehr als 7000 Hotels und Resorts eine der weltweit größten, hat Widerspruch gegen das Bußgeld der ICO angekündigt.

Speicherung der Daten von Bewerbern

Die österreichische Datenschutzbehörde bestätigt die von der UIMC vertretene Meinung: So ist die Speicherfrist von sieben Monaten nach dem Abschluss des Bewerbungsprozesses zulässig (Ö-DSB: 27.08.2018, DSB-D123.085/0003-DSB/2018).

UIMC.austria (eine Marke der UIMC Dr. Vossbein GmbH & Co KG), Fleischmarkt 1/6/12, A-1010 Wien
Tel.: +43 1 20 5107 3383, E-Mail: consultants@uimc.at, Internet: www.UIMC.at

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 Nutzung von Bewerberdaten

☐ **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: www.UIMC.de

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.at widersprechen.