UIMCommunic@tion

01/2019

Ausgabe für Deutschland

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Harter Brexit kann zu Übermittlungsverbot von Daten nach UK führen

Der Brexit ist beschlossene Sache. Fraglich ist allerdings weiterhin, ob das Vereinigte Königreich die Europäische Union nach 46 Jahren Mitgliedschaft über das verhandelte Austrittsabkommen oder ohne eine Vereinbarung (harter Brexit) verlassen wird. Das britische Parlament hat dazu gestern eine Entscheidung getroffen und wird (zumindest vorerst) das Austrittsabkommen nicht annehmen. Für Unternehmen auf dem europäischen Festland mit wirtschaftlichen Verbindungen inklusive Datenverarbeitung eine schwierige Situation. Das Vereinigte Königreich würde bei einem harten Brexit ab 30. März 2019 zu einem datenschutzrechtlichen Drittland aus Sicht der EU (die UIMC berichtete). Der langjährige Datenschutzfachmann Dr. Jörn Voßbein spricht aus, was viele denken: „Diese Situation ist einmalig und verdient deshalb allerhöchste Aufmerksamkeit aller Beteiligten, um Fehler zu vermeiden und Kosten gering zu halten."

In Bezug auf den Brexit sollten deshalb die Vorkehrungen in Unternehmen schnellstmöglich angegangen werden, um im Falle eines „harten Brexits" vorbereitet zu sein. Ein Blick auf ausgewählte Anwendungsfälle der DSGVO für Unternehmen mit Sitz in der EU verdeutlicht die Tiefe der anstehenden Herausforderungen.

Ein zentraler Anwendungsfall ist die Auftragsverarbeitung (AV). Grundsätzlich ist mit dem Dienstleister ein Vertrag über die Auftragsverarbeitung zu schließen, egal ob der Dienstleister innerhalb oder außerhalb der EU ansässig ist. Zusätzlich gilt jedoch folgendes, wenn der Dienstleister außerhalb der EU sitzt (was im Falle eines Brexits für UK-Unternehmen vorliegen würde):

a) Der Verantwortliche oder Auftraggeber kann mit den Empfängern der Daten im UK vertraglich ein bestimmtes Schutzniveau festlegen. Das geschieht auf dem Fundament der sog. **Standardvertragsklauseln**, die die EU-Kommission genehmigt hat. Die Standards müssen mit dem jeweiligen Partner im UK vertraglich geregelt werden. Konkret: sie werden bei bestehenden Verträgen als Nachtrag hinzugefügt oder als „Stand Alone-Agreement" abgeschlossen.

b) **Binding Corporate Rules:** Unterwirft sich ein Konzern verbindlichen internen Daten-schutzvorschriften und werden diese von der zuständigen Aufsichtsbehörde genehmigt, so kann die Datenübermittlung in ein Drittland stattfinden. Vorsicht: es handelt sich um aufwändiges und daher zeitintensives Verfahren. Auch kann dies nur im eigenen Konzern Anwendung finden, sowohl bei einer konzerninternen Auftragsverarbeitung als auch bei einer konzern-internen Datenübermittlung.

Unterauftragnehmer im Rahmen der Auftragsverarbeitung bilden einen weiteren Anwendungsfall, der in den Blick genommen werden muss. Bereits jetzt sollte in einem AV-Vertrag geregelt sein, wie bei der Beauftragung eines Unterauftragnehmers (insbesondere in einem Drittland) durch einen Auftragnehmer zu verfahren ist. Wenn dazu nichts geregelt wurde, liegt der Fall klar: eine Inanspruchnahme von Unterauftragsverarbeitern durch den Auftragsverarbeiter ist ohne schriftliche Genehmigung des Verantwortlichen ausgeschlossen. Falls solche Passagen im AV-Vertrag bzgl. Datentransfers in Drittländer vorhanden sind, sollte eine Konkretisierung für Unterauftragnehmer in dem zukünftigen Drittland UK erarbeitet werden. „Wir empfehlen für zukünftige Verträge mit Dienstleistern, dass jede Art der Verlagerung in ein Drittland der vorherigen Zustimmung des Auftraggebers bedarf und klare Bedingungen der Verlagerung definiert werden", rät Dr. Jörn Voßbein.

Dies bedeutet: Bis zur Anerkennung eines angemessenen Datenschutzniveaus in UK muss die Einhaltung eines angemessenen Datenschutzniveaus beim Datenexport auf andere Weise sichergestellt werden. **Andernfalls müssten zum Stichtag (29. März 2019) alle Datentransfers nach UK beendet werden.**

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

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

UIMC unterstützt <KES> Sicherheitsstudie

Eine getrennte Betrachtung der Themen Informationssicherheit und Datenschutz ist für ein Unternehmen kaum mehr möglich und noch weniger sinnvoll. Dies liegt primär an der generell gestiegenen Bedeutung des Datenschutzes im Zusammenhang mit der Datenschutz-Grundverordnung (DSGVO). Einen eindeutigen Beleg hierfür liefert die Umfrage: Die DSGVO erreichte eine Relevanz von 99 Prozent unter den befragten Unternehmen; sicherlich begünstigt durch eine fortgesetzte mediale Berichterstattung zur Datenschutz-Novelle.

Neben den Veränderungen durch die DSGVO im Feld des Datenschutzes sind die Auswirkungen im Bereich der ISi keineswegs unbedeutender. Der Fall liegt klar: die DSGVO führt im Rahmen der technischen und organisatorischen Maßnahmen zu einer Neuausrichtung. So fordert die DSGVO nicht nur die Erfüllung der klassischen Ziele der ISi, sondern stellt auch Forderungen nach erhöhter Transparenz und regelmäßiger Revision der implementierten Maßnahmen, die stark an ein Informationssicherheits-Managementsystem (ISMS) erinnern. Hieraus ergibt sich der Aufbau eines Datenschutz-Managementsystems im Sinne eines ISMS für personenbezogene Daten. Eine getrennte Betrachtung ist demnach wenig sinnvoll, um keine Synergien durch zwei parallele Systeme zu verlieren.

Die Studie stellt einen wichtigen Impuls für eine Sensibilisierung bei der Verschränkung von Datenschutz und Informationssicherheit dar. **Sie haben Interesse an einem kostenlosen Belegexemplar mit allen Ergebnissen? Dann melden Sie sich einfach bei uns!**

Erste Kontrollen der Datenschutz-Aufsichtsbehörden

Das Bayrische Landesdatenschutzamt (BayLDA) führt im Rahmen seiner gesetzlichen Aufgaben regelmäßig anlassbezogene und anlasslose Datenschutzprüfungen durch. Ferner finden natürlich auch anlassbezogene Prüfungen statt (meist aufgrund von Beschwerden oder konkreten Hinweisen auf mögliche Datenschutzverstöße). Anlasslose Prüfungen erfolgen nach pflichtgemäßem Ermessen branchenunabhängig. Das BayLDA führt diese anlasslosen Prüfungen in der Regel als sog. fokussierte Prüfungen bei einzelnen Unternehmen vor Ort, als Prüfungen im Wege eines schriftlichen Verfahrens oder als Onlineprüfung automatisiert über das Internet durch. Darüber hinaus beteiligt sich das BayLDA auch an überregionalen Prüfungen.

Dies zeigt, dass künftig auch proaktive Kontrollen durchgeführt werden und nicht erst auf eine Beschwerde gewartet werden soll.

Es ist davon auszugehen, dass die weitere Landes-Aufsichtsbehörden diesem Beispiel folgen wird.

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

- ☐ Harter Brexit kann zu Übermittlungsverbot von Daten nach UK führen
- ☐ Teilnahme an der Verlosung für Freikarten zur IT-Trends Sicherheit in Bochum (27.03.2019)
- ☐ **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