07/2013

UIMCommunic@tion

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Der sichere Hafen ist gesperrt!

Der Konzern-interne Datentransfer ist in Folge von PRISM nun erschwert

[Wuppertal, Saarbrücken] Es ist heute allgemein üblich, dass die Datenverarbeitung globalisiert wird. Ob nun innerhalb eines Konzerns oder mit Hilfe von zunehmend weltweit organisierten Dienstleistern, die den Unternehmen Support im „follow the sun"-Prinzip anbieten. Die erforderliche Genehmigung für einen Datentransfer ins außereuropäische Ausland wollen die Datenschutz-Aufsichtsbehörden in Folge des PRISM-Skandals aber vorerst nicht mehr erteilen, was für viele Unternehmen ein z. T. massives Compliance-Risiko darstellen kann.

In vielen (globalen) Konzernen werden Matrix-Organisationen etabliert, IT-Systeme durch spezialisierte Dienstleister rund um die Uhr gewartet oder konzernweite Telefonverzeichnisse erstellt. Aber auch die Vermarktung der Produkte findet zunehmend global statt, so dass auch das Customer-Relationsship-Management (CRM) weltweit im Unternehmensverbund realisiert wird. All dies hat zur Folge, dass personenbezogene Daten auch für andere (rechtlich selbständige) Firmen zugänglich sind.

Im Rahmen des Datenschutzes ist es ausschließlich dann zulässig, personenbezogene Daten (ob über Kunden oder Mitarbeiter) zu übermitteln, wenn hierfür sowohl eine Rechtsgrundlage als auch ein „angemessenes Schutzniveau" beim Empfänger vorliegt. Dies gilt explizit auch für die Mutter-, Tochter- oder Schwestergesellschaft eines Unternehmens, da ein solcher Datentransfer rechtlich nicht privilegiert wird (kein sog. Konzernprivileg).

Sofern ein solcher Datentransfer an ein Unternehmen außerhalb von Deutschland und der EU stattfindet (wie beispielsweise aus den USA), sind durch das datenübermittelnde Unternehmen zusätzliche Vorgaben zu beachten, da in den USA kein dem deutschen oder europäischen herrschenden Datenschutzgesetz existiert. So musste sich beispielsweise das datenempfangende Unternehmen in den USA dem „Safe-Harvor-Abkommen" unterwerfen oder sog. EU-Standardvertragsklauseln abgeschlossen werden. Sobald eines dieser beiden Anforderungen erfüllt wurde, konnte die zuständige Datenschutz-Aufsichtsbehörde eine Genehmigung der Datenübermittlung erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder haben angesichts des Skandals um die umfassende Spionage durch die USA mittels dem Spähprogramm PRISM bekanntgegeben, vorerst keine Genehmigungen mehr für Unternehmen auf Basis des Safe-Harbor-Abkommens zu erteilen. Auch sollen sämtliche einschlägigen Datentransfers auf Grundlage der Standardklauseln geprüft und ggf. ausgesetzt werden.

Somit ist es aktuell kaum möglich, dass deutsche Unternehmen die Daten mit amerikanischen Konzern-Müttern auszutauschen (und sei es nur das Konzern-Telefonbuch), den Support im „Follow-the-Sun"-Prinzip mit ausländischen Dienstleistern zu organisieren oder günstige Cloud-Dienste von Nicht-EU-Anbietern zu nutzen. Vielmehr müssen diese Rahmenbedingungen und die damit verbundenen (prozessualen, finanziellen und personellen) Risiken entsprechend berücksichtigt werden. Dies gilt für internationale Prozesse, IT-Systeme, Vertragsverhältnisse und auch Projekte. Der betriebliche Datenschutzbeauftragte sollte hierbei stets der erste Ansprechpartner sein.

Daher ist die UIMC der Auffassung, dass der Datenschutz in die Verhandlungen zwischen der EU und den USA zum Freihandelsabkommen aufgenommen werden sollte. Andernfalls weder eine sinnvolle Lösung für Unternehmen noch eine angemessene Lösung zum Schutz der Persönlichkeitsrechte der Betroffenen gefunden werden.

Mehr Pressemitteilungen finden Sie hier: www.UIMC.de/communication

Schon gewusst?

Ob hiermit eine Datenübermittlung verbunden ist oder nicht, für jedes „Verfahren" [also mittels Software (teil-) automatisierter Prozess] muss eine **Verfahrensübersicht** erstellt werden. Diese Verfahrensübersicht ist **dem Datenschutzbeauftragten zur Verfügung zu stellen**.

Wir bieten Ihnen hierzu das „computergestützte Verfahrensverzeichnis" (CVV) für alle Rechtsgrundlagen zur vereinfachten Umsetzung:

CVV.UIMC.de

Haben Sie Fragen?
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Noch Fragen?
Treten Sie in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Der sichere Umgang mit Smartphone-Funktionen

Smartphones werden in Unternehmen und Behörden immer alltäglicher. Doch neben all den nützlichen Funktionen bieten Smartphones zunehmend Dienste an, die im privaten Umfeld noch aktzeptabel sind oder der Nutzer dies zumindest für sich selbst entscheiden kann, aber für den dienstlichen Gebrauch problematisch sind. Aus diesem Grunde sollten u. a. folgende Aspekte beachtet werden:

1. Dienstliche E-Mails, Termine und Adressen sollten ausschließlich mit von der Firmen-IT bereitgestellten Diensten und Programmen synchronisiert werden.
2. Synchronisierungen von geschäftlichen (Kontakt-) Daten mit Diensten im Internet (beispielsweise „Freunde-Finder“ von sozialen Netzwerken) sollten untersagt/unterbunden werden.
3. Internet-Speicherdienste und andere Anlagedienste (z. B. iCloud, Google Services oder Dropbox) sollte für dienstliche Zwecke nicht verwendet werden.
4. Es sollten ausschließlich von der IT freigegebene Apps installiert und das Herunterladen nur aus offiziellen Quellen (z. B. Apple Appstore oder Google Play Store) zugelassen werden!
5. Die Nutzung von öffentlichen WLAN-/Wifi-Netzen (z. B. Hotspots in Hotels, Cafes oder Flughäfen) sollte grundsätzlich verboten werden.
6. Schnittstellen wie Bluetooth, Infrarot oder NFC sollte bei Nichtbenutzung ausgeschaltet werden. Gleiches gilt für etwaige Ortungsdienste.

Weitere Hinweise zur sicheren Nutzung von Smartphones haben wir übrigens schon in der Ausgabe 01/2013 gegeben.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Auszug aus bisher erschienenen Hinweisen/Tipps:
„Der richtige Umgang mit Besuchern“ (06/13)
„Clean Desktop Policy“ (05/13)
„Beantwortung telefonischer Auskünfte“ (03/2013)
„Nutzung von sozialen Netzwerken“ (02/2013)

Praxis-Workshop

In vielen Datenschutzgesetzen wird eine formale Vorabkontrolle eines neuen IT-Systems gefordert. Doch auch in Bereichen, wo dies nicht explizit gefordert wird, so doch mindestens implizit: So sollte eine neue Software stets nur dann eingesetzt werden, wenn zuvor die rechtlichen und technischen Vorgaben entsprechend „vorab kontrolliert“ wurden. **Informieren Sie sich über pragmatische Herangehensweisen.**

25.09.2013, Wuppertal

Wünsch dir was!

Wenn Sie im Rahmen der UIMCommunication über ein bestimmtes Thema einmal informiert werden möchten, dann kommen Sie auf uns zu. Ob Hintergrund-Informationen, Tipps und Hinweise oder Unterstützungswerkzeuge zum Datenschutz oder zur Informationssicherheit: Gerne können Sie ein Wunschthema an die Redaktion der Informationsbriefs der UIMC/UIMCert richten.

communication@uimc.de

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

- ☐ Der Konzern-interner Datentransfer ist in Folge von PRISM nun erschwert
- ☐ Computergestütztes Verfahrensverzeichnis (CVV)
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de