UIMCommunic@tion

06/2016

Ausgabe für Österreich

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Bei Ausgründung Datenschutz nicht vergessen!

Eine Unternehmensausgründung birgt eine Menge Herausforderungen. Über tarif- und steuerrechtliche Fragestellungen darf der Datenschutz aber nicht vergessen werden. „Oftmals geht es bei einem Ausgründungsprozess um personenbezogene Daten, die schutzbedürftig sind", weiß Datenschutzexperte Dr. Jörn Voßbein aus Erfahrung. Um die Bestimmungen des Datenschutzrechtes einzuhalten, ist ein seriöses Vorgehen erforderlich. „Aber die Wahrung des Datenschutzes ist machbar und sicher kein Hexenwerk."

Wirft man einen Blick auf die Definition des betriebswirtschaftlichen Begriffes ‚Ausgründung', findet sich z. B. im Gabler Wirtschaftslexikon Folgendes: „Überführung eines Teilbetriebs oder eines Betriebsteils […] in eine dafür neu gegründete Gesellschaft." Was gilt es hierbei aus Sicht des Datenschutzes zu beachten?

Daten von Beschäftigten, die in das ausgegründete Unternehmen wechseln, dürfen grundsätzlich beim Übergang in das neue Unternehmen übermittelt werden. Eine Prüfung dieser Aussage ergibt die Rechtmäßigkeit eines solchen Handelns, weil personenbezogene Daten eines Beschäftigten für die Zwecke eines Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden dürfen. Aber: Daten von Mitarbeitern, die im bisherigen Unternehmen verbleiben, dürfen auf Basis dieser Rechtsgrundlage nicht übermittelt werden. Gerade eine exakte Trennung zwischen den Daten vom Betriebsübergang betroffener und nicht betroffener Mitarbeiter kann in der gelebten Praxis zu Schwierigkeiten führen. Im Grundsatz liegen drei Gruppen von Daten vor:

a) Eindeutig einer Person zugeordnete und separat abgelegte Daten/Unterlagen – Beispiel: Personalakten.

b) Daten, die einer Person zugeordnet werden können, aber nicht systematisch nach Personen angelegte Dateien oder Unterlagen – Beispiele: elektronische Korrespondenz oder Datenbanken.

c) Listen und Aufstellungen von Mitarbeitern – Beispiel: Teilnehmerlisten

Eine vollkommen datenschutzkonforme Lösung kaum umsetzbar ist, da es sich nicht vermeiden lässt, dass auch Mischdaten im neuen Unternehmen ankommen. Dr. Jörn Voßbein bezieht hierzu klar Stellung: „Zielsetzung muss es bei einer Ausgründung daher sein, so datenschutzkonform zu arbeiten, wie möglich." Das Ziel ist mit Bewusstsein für den Datenschutz, Sensibilität beim Umgang mit personenbezogenen Unterlagen und rechtzeitiger und konsequenter Datentrennung unter Risikogesichtspunkten erreichbar.

Ausführliche Informationen finden Sie unter communication.uimc.de

Was bedeutet der Brexit für den betrieblichen Datenschutz?

Am 23. Juni 2016 hat die Bevölkerung von Großbritannien im Rahmen eines Referendums entschieden, aus der Europäischen Union (EU) auszuscheiden. Auch wenn die britische Regierung noch nicht final beschlossen hat, ob sie sich an den „Volkswillen" halten will, stellen schon jetzt viele Unternehmen, die wirtschaftliche Beziehungen zu Unternehmen in Großbritannien haben, die Frage nach den Konsequenzen im Hinblick auf den Datenschutz. Dr. Jörn Voßbein, mehrfach bestellter Datenschutzbeauftragter, ist aber wenig beunruhigt.

Im Rahmen von Dienstleistungen oder Konzern-Verflechtungen finden bei vielen österreichischen und anderen europäischen Unternehmen Datentransfers nach Großbritannien statt. Bislang war dies relativ unproblematisch, schließlich sind die britischen Länder Teil der EU, so dass ein angemessenes Datenschutzniveau vorliegt. Doch wie sieht dies aus, wenn der „Brexit" auch Realität wird.

Zwar erfolgt die Prüfung einer grenzüberschreitenden Datenübermittlung generell zweistufig. So müssen zunächst die Anforderungen einer Datenverarbeitung als solches erfüllt sein und es ist darüber hinaus zu prüfen, ob beim Empfänger ein angemessenes Datenschutzniveau sichergestellt ist. Doch wird innerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) – bereits aufgrund der vorhandenen europarechtlichen Vorgaben – das Vorhandensein eines angemessenen Datenschutzniveaus unwiderleglich angenommen. Der Einsatz von britischen Dienstleistern (z. B. Data Centre, Remote Support) oder die Nutzung von „Shared Services" bei britischen Konzerngesellschaften unterlag den gleichen Anforderungen wie im Inland.

Bei einem Datentransfer nach Großbritannien kann nach einem potentiellen Austritt nicht mehr per se davon ausgegangen werden, dass ein angemessenes Datenschutzniveau existiert. **Was bedeutet dies nun für die Übermittlung von personenbezogenen Daten?**

Der Brexit hat zumindest aktuell im Hinblick auf den Datenschutz noch keine Konsequenzen für Unternehmen in Österreich. Die weiteren Vorgehensweisen von EU und Großbritannien sollten aber dringend mitverfolgt werden, um möglichst frühzeitig etwaige Maßnahmen zu ergreifen.

Ausführliche Informationen finden Sie unter communication.uimc.de

UIMC Dr. Vossbein GmbH & Co KG, Nützenberger Straße 119, 42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0, 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

Locky: Sicherer Umgang mit dem Internet und Mail-Anhängen

In der letzten Zeit haben wieder einmal verschiedene Vorkommnisse gezeigt, dass das Thema „Malware“ (Viren, Trojaner, Ramsonware etc.) noch immer aktuell ist. Mittels „Locky“ wurden IT-Systeme verschlüsselt und die Besitzer sollten eine „Lösegeldzahlung“ leisten, um wieder an die Daten zu gelangen.

Nachfolgend möchten wir ein paar Hinweise geben, um die Gefahr einer Infektion zu reduzieren:

» **Erstellung von Backups** [da gespiegelte Platten ebenfalls infiziert werden können, sollten auch regelmäßig separate Datenträger mit Datensicherungen im Mehr-Generationen-Prinzip erstellt werden]

» **Aktualisierung von Systemen** [Betriebssystem, Office-Produkte, Virenschutzprogramme, Mail-Programm, Browser und Plug-ins (zeitnah nach Erkennen von Sicherheitslücken und nach Veröffentlichung durch den Hersteller)]

» **Blockierung von aktiven Inhalten** [Office-Produkte und Browser so konfigurieren, dass andere aktive Inhalte erst nach Rückfrage ausgeführt und das automatische Nachladen aus dem Internet verhindert werden (beispielsweise in E-Mails im HTML-Format)]

Darüber hinaus sollten die **User** über folgende Punkte **informiert und senisibilisiert** werden:

» Mail-Anhänge sind nur dann zu öffnen, wenn diese von einer **vertrauenswürdigen Person** übersandt wurden. Im Zweifelsfall sollte telefonisch nachgefragt werden, ob die E-Mail tatsächlich versandt wurde. Analoges gilt für externe Datenträger, wie z. B. USB-Sticks).

» Sofern die Vertrauenswürdigkeit des Versenders nicht sichergestellt ist, sollte einem Link in einer E-Mail nicht gefolgt werden.

» ZIP-Dateien, Dateien mit ausführbaren Codes (beispielsweise Makro) usw. sind mit besonderer Vorsicht zu betrachten. Bei der „Aufforderung“, aktive Inhalte zu aktivieren (beispielsweise im Browser, Word- oder Exceldokumenten), sollte dies nur bei der **Vertrauenswürdigkeit** von Absender und Datei getan werden.

» Im Zweifelsfall sollte stets der **Administrator** oder den Versender gefragt werden.

Aktuelles aus Österreich und der Welt

Datenschutz-Splitter

Standardvertragsklauseln sollen vor EuGH auf Rechtmäßigkeit geprüft werden

Erneute Datenpannen im Internet (aktuell: Twitter aufgrund eines Browser-Bug)

Millionenklage eines Fotografen aufgrund verletzter Urheberrechte

ZEW-Studie: Insbesondere Gratis-Apps haben zu umfassenden Zugriff auf sensible Daten

Save the date

Quo vadis, Datenschutz?

Im Rahmen des DHK Lunch der Österreichischen Auslands-Handelskammer werden wir innerhalb eines Vortrags nicht nur die geänderten (rechtlichen) Rahmenbedingungen, sondern auch pragmatische Lösungsansätze (insbesondere für KMU) in Folge der EU-Datenschutz-Grundverordnung skizzieren.

Grand Hotel Wien, 13.09.2016

Bei Interesse kommen Sie gerne auf uns zu.

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

☐ Bei Ausgründung Datenschutz nicht vergessen!

☐ Was bedeutet der Brexit für den betrieblichen Datenschutz?

☐ **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) 265 74 - 19 oder formlos per Mail an communication@uimc.de

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

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