11/2014

UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Nicht im Sinne der Datenschutz-Aufsichtsbehörden:

Auftragsdatenverarbeitung: Kein Audit ist auch keine Compliance-Lösung

Sobald personenbezogene Daten durch einen Dienstleister verarbeitet werden (bzw. ein Zugriff hierauf nicht auszuschließen ist), muss sich der Auftraggeber von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen. Ein solcher Check stellt viele Unternehmen nicht selten vor eine Herausforderung. Zum einen fehlt ein geeigneter Fragenkatalog, nach dem diese Überprüfung vorgenommen werden soll, zum anderen fehlt oft eine effiziente Methodik, z. T. auch die Fachkompetenz und sehr oft ausreichend Zeit, um ein solches Audit vorzubereiten, durchzuführen und die Ergebnisse auszuwerten.

Innerhalb des § 11 Bundesdatenschutzgesetz (BDSG) sind Unternehmen dazu verpflichtet, nicht nur die Verträge entsprechend der gesetzlich vorgegebenen Inhalte zu gestalten (wie z. B. zu Sicherheitsmaßnahmen oder Kontrollrechten), sondern auch die Outsourcing-Dienstleister im Hinblick auf die Umsetzung der vorgegebenen Sicherheitsmaßnahmen zu überprüfen. Diese Prüfung muss nicht nur vorab im Rahmen des Auswahlverfahrens durchgeführt, sondern auch danach regelmäßig wiederholt werden. Auch eine Dokumentation dieser Prüfung ist gesetzlich verpflichtend.

Diese Vorgaben gelten im Übrigen nicht nur bei einer aktiven Datenverarbeitung (wie z. B. Personalabrechnung, Digitalisierung von Rechnungen und Lettershop), sondern auch für den IT-Support beispielsweise durch Fernwartung, wenn dabei „ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann“. Hierbei wird oft auch vergessen, dass das BDSG keine Privilegierung von Konzerngesellschaften wie Mutter-/Tochter-Unternehmen vorsieht und diese Unternehmen genauso wie externe Auftragnehmer behandelt werden müssen.

Für die Durchführung dieser Kontrollanforderungen fehlt vielen Unternehmen nicht nur die fachliche, sondern auch die methodische Kompetenz sowie die Erfahrung zur Durchführung dieser Audits. Viele ignorieren diese gesetzliche Pflicht, was Datenschutz-Aufsichtsbehörden bemängeln.

Andere Unternehmen greifen auf „Profis“ zurück, die oftmals schneller und routinierter vorgehen können. So haben diese beim Auftragnehmer auch oftmals eine höhere „Autorität“ als der Auftraggeber bzw. Kunde selbst, wie Dr. Heiko Haaz (Leiter der Datenschutz-Zertifizierungsstelle der UIMCert GmbH) berichtet. Diese verbessert die Akzeptanz der Befragung und Ergebnisse; auch beim Dienstleister selbst.

Ein zusätzlicher Vorteil ist, dass solche Auditierungen auch koordiniert werden können, indem weitere Kunden des Dienstleisters angesprochen und von einer gemeinsamen Auditierung überzeugt werden. Der Dienstleister hat somit nur ein Audit zu „ertragen“ und die verschiedenen Auftraggeber können die Kosten und Aufwände aufteilen, so dass erhebliche Kosteneinsparungen möglich sind.

Das Ergebnis sollte nicht nur ein Status-Quo-Bericht sein, sondern auch einen Maßnahmenkatalog mit Vorgaben an den Dienstleister zur Verbesserung enthalten. Dies verbessert nicht nur den Datenschutz, sondern auch allgemein die Qualität der Dienstleistung.

Dienstleister selbst könnten dabei sogar noch einen Schritt weitergehen und sich zertifizieren oder testieren lassen. So kann ein Gütesiegel, wie beispielsweise das von der UIMCert, einen hohen Qualitätsstandard proaktiv gegenüber (potentiellen) Kunden dokumentieren. Dies ist nicht nur eine vertrauensbildende Maßnahme, sondern kann auch Kunden-Audits ersetzen oder zumindest reduzieren.

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

Schon gewusst?

Nicht nur durch die Bereitstellung, sondern auch durch die **Nutzung eines öffentlichen Hotspots** erhöht sich (neben den gewohnten Risiken, die jede Internetverbindung birgt) die Gefahr für Vertraulichkeit und Integrität der Daten. Auch wenn es natürlich keine 100%ige Sicherheit geben kann, sollten (ob nun beim privaten oder dienstlichen Gebrauch) **entsprechende Sicherheitsmaßnahmen** ergriffen werden, um die Informationen auf dem Gerät und beim Transfer zu schützen.

Fragen Sie Ihren IT-Sicherheitsbeauftragten

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 mit uns in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Einführung einer Matrix-Organisation

Gerade in Unternehmensverbünden werden zunehmend Matrix-Organisationsstrukturen etabliert. Hierdurch findet eine Datenübermittlung im Sinne des Datenschutzes statt, für die eine explizite Rechtsgrundlage erforderlich ist.

Sofern die Verarbeitung personenbezogener Daten zur Erfüllung des Arbeitsvertrags erforderlich sind, dürfen diese Daten gemäß § 32 BDSG übermittelt werden. **Tipp:** Hierzu muss innerhalb des Arbeitsvertrags ein direkter Konzernbezug enthalten sein.

Falls der Konzernbezug fehlt, werden im Folgenden die Anforderungen der Datenschutz-Aufsichtsbehörden kurz dargestellt (innerhalb der EU und EWR):

- Keine willkürliche Erweiterung des Verarbeitungsumfangs als zu Zwecken des Arbeitsverhältnisses
- Keine größeren **Befugnisse** einer anderen Konzerngesellschaft als die des Arbeitgebers
- Keine Bildung eines frei verfügbaren Datenpools
- **Transparenz** durch angemessene Information des Arbeitnehmers über die Übermittlung (E-Mail kann ausreichend sein)
- **Interessenabwägung** in jedem Einzelfall, da die arbeitsteilige Zusammenarbeit im Konzern nicht per se höher als die schutzwürdigen Interessen des Betroffenen anzusehen sind
- Wahrung des fehlenden Konzernprivilegs
- Konzernweit einheitliches **Datenschutzkonzept** (Schaffung, Erhaltung und Durchsetzung der Datenschutzrechte der Betroffenen und abgestimmte Sicherheitsmaßnahmen)
- Arbeitgeber bleibt trotz Diversifizierung der Verantwortlichkeit weiterhin uneingeschränkter Ansprechpartner für den Arbeitnehmer
- **Verbindliche Regelung** zwischen beteiligten Konzernunternehmen (Verträge oder verbindliche Konzernregeln)
- Verbindlichkeit der **Regelungen gegenüber Betroffenen** (z. B. durch einen Vertrag zugunsten Dritter oder durch eine Konzern-Betriebsvereinbarung).

Mehr Informationen zu diesem komplexen Thema erhalten Sie bei Ihrem Ansprechpartner bei der UIMC!

Stärkung der Sensibilisierung im eCollege

Das eCollege wird ein Update erhalten, welches stärker multimediale Elemente aufnimmt. Die Erzählung von typischen Szenen und Vorfällen aus dem betrieblichen Alltag in kleinen Geschichten/Filmsequenzen führt zu einer hohen Identifikation mit dem Thema (mit und ohne Audio). Somit wird die Sensibilisierung der Mitarbeiter in Fragen des Datenschutzes und der Sicherheit von Informationen noch weiter gestärkt.

Mehr zum eCollege unter

eCollege.UIMC.de

UIMC/UIMCert-Informationstage 2014

Die Datenschutzfachtagung (DAFTA) findet jährlich im Maternushaus in Köln statt. Als eines der marktführenden Unternehmen ist die UIMC mit der UIMCert auch dieses Jahr vor Ort. Hier können Sie in gemütlicher Atmosphäre nicht nur mit uns fachsimpeln, sondern sich auch über unser aktualisiertes eCollege zur Sensibilisierung der Mitarbeiter oder unsere Kampagne zur Dienstleister-Auditierung informieren.

Wir freuen uns auf Ihren Besuch:

Köln, 19./20.11.2014

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

- Auftragsdatenverarbeitung: Kein Audit ist auch keine Compliance-Lösung
- Gefahren bei der Nutzung eines öffentlichen Hotspots
- **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