UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Was tun, wenn der Kunde nach Datenschutz fragt?

Nicht nur im Rahmen des Endkundengeschäfts, sondern auch bei klassischen Dienstleistungen zwischen Unternehmen wird zunehmend die tatsächliche Umsetzung des Datenschutzes beim Dienstleister kritisch hinterfragt. Dies kommt einerseits aus der gestiegenen Sensibilisierung zum Datenschutz und zur Informationssicherheit im Zuge der NSA-Affäre („Sind meine Daten sicher?"). Andererseits ist es aber auch darin begründet, dass der Gesetzgeber explizite Vorgaben zur Gestaltung dieser Zusammenarbeit vorgegeben hat und verschiedene Aufsichtsbehörden nun auch dazu übergehen, dies zu prüfen. So sind entsprechende Anforderungen vertraglich zu fixieren und regelmäßige Audits beim Auftragnehmer durchzuführen; im Zweifel auch bei der Muttergesellschaft.

Spätestens seit der Novelle des Bundesdatenschutzgesetzes (BDSG) im Jahre 2009 wurde eine Vielzahl von Unternehmen vor die Herausforderung gestellt, die Compliance-Situation ihrer Dienstleistungsverhältnisse auf Basis des § 11 BDSG neu zu gestalten. So müssen die Verträge gesetzlich vorgegebene Inhalte enthalten (wie z. B. zu Sicherheitsmaßnahmen oder Kontrollrechten); ferner müssen die Outsourcing-Dienstleister im Hinblick auf die Umsetzung der vorgegebenen Sicherheitsmaßnahmen überprüft werden. Diese Prüfung muss nicht nur vorab im Rahmen des Auswahlverfahrens durchgeführt, sondern auch danach regelmäßig wiederholt werden. Auch eine Dokumentation dieser Prüfung ist Pflicht.

Diese Vorgaben gelten nicht nur für das Outsourcing der Personalabrechnung, der elektronischen Archivierung und des Lettershops, sondern auch für den IT-Support beispielsweise durch Fernwartung auf dem Kunden-System, wenn dabei „ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann". Hierbei wird jedoch oftmals vergessen, dass das BDSG keine Privilegierung von Konzerngesellschaften wie Mutter-/Tochter-Unternehmen vorsieht und diese Unternehmen genauso wie externe Auftragnehmer behandelt werden müssen.

Auf der anderen Seite sehen sich viele Dienstleister damit konfrontiert, dass sie von einer Vielzahl ihrer Kunden auf das Thema Datenschutz angesprochen werden. Somit müssen diesbezüglich einerseits intern (revisionssichere bzw. prüfbare) Strukturen und Prozesse geschaffen werden, um eine ausreichende Qualität sicherstellen zu können. Ein Qualitätsmanagementsystem ist zwar sehr häufig umgesetzt, eine explizite Berücksichtigung von datenschutzrechtlichen Anforderungen ist nach Erfahrungen der UIMC aber nicht die Regel, sondern vielmehr die Ausnahme. Es müssen jedoch klare Regeln zu den Berechtigungen auf die Kundendaten und -systeme, zur Verpflichtung und Sensibilisierung der Mitarbeiter, aber auch zu weiteren technischen und organisatorischen Maßnahmen getroffen werden. Idealerweise sollte der Datenschutzbeauftragte hierbei eine zentrale Rolle einnehmen. Andererseits werden die Dienstleister durch die Auftraggeber auditiert, ob die vorgenannten Regeln existieren und auch umgesetzt sind.

Um nicht gänzlich unvorbereitet zu sein, sollte der Dienstleister neben den verbindlichen Regeln auch selbst einmal ein solches Audit intern durchgeführt haben. Anhand eines etablierten Fragenkatalogs kann die eigene Organisation dahingehend geprüft werden, ob die rechtlichen Anforderungen erfüllt sind oder umfassende Nachbesserungsforderungen durch den Kunden drohen. Wenn das interne Audit durch einen externen Auditor vorgenommen wird, gewinnt dies an Objektivität und Neutralität. Durch die „geliehene Autorität" können bestimmte Vorhaben zielführender angestoßen und umgesetzt werden, schließlich hat es „der Prophet im eigenen Land" stets schwerer. Eine solche Auditierung mit externer Unterstützung kann wiederum auch für externe Zwecke genutzt werden, indem die Ergebnisse dem (potenziellen) Kunden zur Verfügung gestellt werden. Auch eine Testierung oder Zertifizierung ist denkbar, wodurch nicht nur zeitintensive Auseinandersetzung mit vielen individuellen Audit-Anfragen entbehrlich werden, sondern auch ein Vertrauensaufbau beim (potenziellen) Kunden stattfinden kann.

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

Schon gewusst?

Gemäß § 11 Absatz 2 BDSG ist ein Dienstleister im Rahmen einer Auftragsdatenverarbeitung (z. B. IT-Systemhaus, Personalabrechnung oder Lettershop) vor Beginn der Dienstleistung und sodann **regelmäßig zu prüfen**, ob die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG eingehalten werden. Dies ist laut BDSG zu **dokumentieren**.

Doch wie umsetzen? UIMC und UIMCert können Sie hierbei mit Konzepten, mit Auditoren und mit Tools unterstützen. **Mehr unter:**

Audit.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?
Kommen Sie auf uns zu!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Fernwartung durch einen externen Dienstleister: Was zu beachten ist

Durch die Fernwartung können viele Dienstleistungen schneller, flexibler und kostengünstiger übernommen werden, da eine Vor-Ort-Präsenz nicht erforderlich ist. Dies stellt natürlich auch ein Risiko dar, schließlich kann nun ein „Betriebsfremder" auf zum Teil vertrauliche Informationen zugreifen.

Der Dienstleister ist sorgfältig **auszuwählen**:

1. Erstellung eines Pflichtenhefts unter Berücksichtigung von Datenschutz und Informationssicherheit (binden Sie schon in dieser Phase den Datenschutzbeauftragten ein);
2. Nachweis der Einhaltung der o. g. Anforderungen (idealerweise durch Vorlage von dokumentierten Konzepten oder Zertifikaten);
3. Abschluss eines Vertrags mit detaillierten Anforderungen (siehe rechte Spalte);
4. Durchführung eines Audits beim Dienstleister zur Überprüfung o. g. Anforderungen.

Innerhalb des **Vertrags** ist u. a. zu regeln (im Übrigen auch, wenn der Dienstleister eine Konzerngesellschaft ist!):

1. Tätigkeiten sind nur nach Weisungen des Auftraggebers bzw. gemäß SLA durchzuführen.
2. Das Wartungspersonal sollte namentlich bekannt sein (möglichst geringe Anzahl). Diese sind auf Datenschutz und Vertraulichkeit zu verpflichten.
3. Idealerweise sollte der Verbindungsaufbau erst durch Auftraggeber explizit freigegeben werden.
4. Sämtliche Wartungsvorgänge sind anhand eines Wartungsprotokolls nachvollziehbar zu gestalten; diese sind regelmäßig zu kontrollieren.
5. Schwachstellen, Vorfälle und sonstige Probleme sind unverzüglich zu melden.

Dies stellt nur einen Auszug dar; weitere Regelungen können Sie bei Ihrem Ansprechpartner erfragen.

Auszug aus bisher erschienenen Hinweisen/Tipps:
„Der richtige Umgang mit Besuchern" (06/2013)
„Tipps zum sicheren, datenschutzkonformen Einsatz von Fernwartungs-Tools" (04/2013)

Vortrag für Dienstleister

Sofern Sie Dienstleistungen anbieten, müssen Sie intern Strukturen schaffen, um einen ausreichenden Datenschutz zu erreichen. Auch müssen Sie sich auch auf Audits vorbereiten, wozu der Kunde gesetzlich verpflichtet ist. Im Vortrag werden wir Anforderungen, Potenziale und pragmatischen Lösungsmöglichkeiten darstellen. Hierbei können wir aufgrund der Betreuung vieler Dienstleister auf diverse Beispiele aus der Praxis zurückgreifen.

13.03.2014, Nürnberg

Workshop für Auftraggeber

In unserer Reihe von Praxis-Workshops widmen wir uns als nächstes dem Thema „Outsourcing". Mit der Auslagerung können z. B. **Personalabrechnung** oder IT-Support oft qualitativ besser und kostengünstiger umgesetzt werden. Dies birgt aber auch Risiken.

In unserem Workshop wollen wir dies und auch Lösungsansätze zum (rechts-) sicheren Outsourcing mit Ihnen diskutieren.

09.04.2014, Wuppertal

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

- ☐ Was tun, wenn der Kunde nach Datenschutz fragt? (Anforderungen an Unternehmens-Dienstleister)
- ☐ Gesetzliche Verpflichtung zur Dienstleister-Auditierung
- ☐ **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