01/2016

UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Die UIMC kann beruhigen:

Nicht jedes Unternehmen betrifft die Vorratsdatenspeicherung

Trotz scharfer Kritik wurde das „Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten" verabschiedet. Hierin ist auch die umstrittene Vorratsdatenspeicherung geregelt. Viele Unternehmen stellen sich nun die Frage, ob diese Regelung, welche im Dezember 2015 in Kraft getreten ist, auch sie betreffen. Die UIMC kann beruhigen.

Entsprechend der neuen Regelungen sind Verbindungsdaten zu speichern, die sich aus den Umständen der Telekommunikation ergeben. Der Inhalt der Kommunikation oder Daten über aufgerufene Internetseiten dürfen nicht gespeichert werden. Für Unsicherheit sorgt die Definition des Kreises der zur Speicherung Verpflichteten.

Gemäß Telekommunikationsgesetz (TKG) richten sich die Speicherpflichten an diejenigen, die öffentlich zugängliche Telekommunikationsdienste erbringen. Nicht in den Anwendungsbereich der Regelung fallen zum Beispiel Betreiber von Krankenhäusern, Hotels oder Gaststätten, die ihren Patienten oder Kunden eine Telefon- oder Internetnutzung lediglich vorübergehend zur Verfügung stellen. Auch wenn Unternehmen externen Besuchern oder Kunden ihre betrieblichen Kommunikationsmittel zur Verfügung stellen, dürfte es sich in der Regel um ein nur vorübergehendes Angebot handeln.

Darüber hinaus stellt sich für viele Arbeitgeber die Frage, ob sie zur Vorratsdatenspeicherung verpflichtet sind. Dies gilt insbesondere vor dem Hintergrund, dass sie durch eine Erlaubnis zur Privatnutzung betrieblicher Kommunikationsmittel (Telefon, Internet, E-Mail) ohne weiteres zum Diensteanbieter im Sinne des TKG werden. Zur Vorratsdatenspeicherung ist jedoch nur derjenige Diensteanbieter verpflichtet, der sog. „öffentlich zugängliche" Telekommunikationsdienste erbringt.

Zwar gibt es keine gesetzliche Definition für den Begriff der „Öffentlichkeit", doch ähnlich etwa dem Versammlungsrecht impliziert der Begriff das Vorhandensein eines unbestimmten Personenkreises (also jedermann). Ein solcher liegt bei der (dienstlichen oder privaten) Nutzung der Telekommunikationsdienste durch die Arbeitnehmer jedoch gerade nicht vor. Die Identität der Mitarbeiter ist dem Unternehmen bekannt; zudem setzt die Nutzung der Telekommunikationsdienste ein eigenständiges Rechtsverhältnis zwischen Arbeitgeber und Arbeitnehmer voraus. Insofern ist davon auszugehen, dass selbst bei erlaubter Privatnutzung von Telefon oder Internet für den Arbeitgeber aus diesem Gesichtspunkt heraus keine Verpflichtung zur Vorratsdatenspeicherung besteht. Analoges gilt für die o. g. Gastzugänge in Hotels, Krankenhäusern oder anderen Unternehmen.

In den aufgeführten Fällen ist ergänzend zu berücksichtigten, dass durch konkrete Sicherheitsvorkehrungen und Beschränkungen – sei es durch die Auswahl der Berechtigten, den Abschluss expliziter Benutzervereinbarungen etc. – ein Ausschluss der Öffentlichkeit sichergestellt werden muss. Sofern keinerlei Beschränkungen gegen die Nutzung durch Externe getroffen werden, droht ansonsten die Einstufung als „öffentlich zugänglicher Telekommunikationsdienst". Zwar sollte bereits aus datenschutz-/haftungsrechtlichen Gründen (sog. „Störerhaftung") eine Absicherung des Netzes bzw. eine Kontrolle der Zugangsberechtigungen erfolgen, spätestens vor dem Hintergrund einer drohenden Verpflichtung zur Vorratsdatenspeicherung dürfte jedoch nun ein entsprechender Anreiz für die Umsetzung der erforderlichen Maßnahmen bestehen.

Schon gewusst?

Hat der Arbeitgeber die private Nutzung von Internet, E-Mail und/oder Telefon erlaubt oder nicht explizit verboten und kontrolliert, so gelten die Vorschriften des TKG und TMG. Als TK-Anbieter hat er das Fernmeldegeheimnis nach § 88 TKG zu beachten. Der Erlaubnisrahmen für die Verarbeitung der Verbindungs-, Nutzungs- und Abrechnungsdaten ist sehr eng gesteckt. Auch Vertretungs- und Nutzungsregeln im Rahmen der E-Mail-Nutzung (z. B. Weiterleitung oder Einsichtnahme im Krankheits-, Urlaubs- oder Kündigungsfall) bergen große Gefahren. Demnach sollte die Nutzung reglementiert werden. Und wie?

Fragen Sie Ihren Datenschutzbeauftragten

UIMC® | in Datenschutz und Informationssicherheit stets gut beraten!

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

Reduktion der Mitstörer-Haftung

Viele Unternehmen bieten Ihren Gästen und Besuchern einen Internet-Zugang an (z. B. WLAN-Hotspot). Sofern durch den Nutzer bspw. Urheberrechtsverletzungen, wird eine Abmahnung in erster Linie an den Anschlussinhaber versendet.

Ein Anschlussinhaber, der selbst keine Urheberrechtsverletzung begangen hat, kann zwar strafrechtlich nicht als Täter im Sinne des Strafrechts in Anspruch genommen werden. Er kann aber zivilrechtlich als Mitstörer/Störer in Anspruch genommen werden, wenn er in irgendeiner Weise willentlich und ursächlich zur Verletzung des geschützten Rechts beiträgt. Ein Anschlussinhaber kann also dann als Störer in Anspruch genommen werden, wenn er seine Prüfpflichten verletzt hat.

Diese Prüfpflichten sind weder durch den Gesetzgeber noch durch eine Rechtsprechung einheitlich definiert. Nichtsdestotrotz hat sich das nachfolgende Vorgehen etabliert. Im Rahmen eines Gast-WLANs, welches Besuchern angeboten wird, kann die Gefahr der Störer-/Mitstörer-Haftung demnach wie folgt reduziert werden:

- Eingrenzung des Nutzerkreises durch die Vergabe von Zugangsberechtigungen:
  - Erforderlichkeit der Authentifizierung des User und
  - Konfiguration von restriktiven Port-Freigaben (um illegale Aktivitäten zu erschweren)
- Nutzerregelungen für die User: Diese sind durch den User entweder schriftlich oder durch das Bestätigen eines „Buttons“ bei der Anmeldung zu bestätigen.

Ferner ist es zu empfehlen, einen dedizierten Zugang zum Internet technisch einzurichten. Hierdurch kann das interne Netzwerks vor unberechtigten Zugriffen geschützt werden.

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

Wünschen Sie sich Tipps oder Wissenswertes zu einem bestimmten Thema? Dann schicken Sie uns eine Mail an communication@uimc.de.

Update: EU-Datenschutz-Grundverordnung

Während der zweijährigen Übergangsphase wird Sie die UIMC über die neuen Anforderungen informieren und bei der Umsetzung mittels hierfür entwickelten UIMChange-Programms tatkräftig unterstützen. Näheres hierzu finden Sie in der UIMCommunication 10/2015. Aktuell sind zunächst **keine Aktivitäten** bei Ihnen erforderlich (Audits, Fortbildungen etc.).

Seien Sie beruhigt:

Wir werden Sie rechtzeitig umfassend informieren!

Seminar: Datenschutz im Gesundheitswesen

Im Rahmen der ambulanten und stationären Krankenversorgung werden besonders sensible Daten erhoben, verarbeitet und genutzt. Die Datenverarbeitung dient nicht nur dem Behandlungsteam als Gedächtnisstütze im Behandlungsprozess, sie wird dem Patienten auch als Nebenpflicht aus dem Behandlungsvertrag geschuldet.

Nutzen Sie unser Seminar zur Fortbildung

Wuppertal, 26.02.2016

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

- ☐ Nicht jedes Unternehmen betrifft die Vorratsdatenspeicherung
- ☐ Risiken durch die fehlende Regelung der Privatnutzung durch den Arbeitgeber
- ☐ **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