WIRTSCHAFTSKAMMER ÖSTERREICH

Wiedner Hauptstraße 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-233
E rp@wko.at
W http://wko.at

Herrn
MR Dr. Christian Singer
Bundesministerium für Verkehr,
Innovation und Technologie
Sektion III, Abteilung PT2
Ghegastraße 1
1030 Wien
JD@bmvit.gv.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen/Sachbearbeiter	Durchwahl	Datum
BMVIT-630.326/0002-III/PT2/2011	Rp 447.0004/2011/WP/VR	4002	20.9.2011

Datensicherheitsverordnung TKG-DSVO (zur Vorratsdatenspeicherung) - Stellungnahme

Sehr geehrter Herr Ministerialrat,

die Wirtschaftskammer Österreich nimmt zum Entwurf für eine Datensicherheitsverordnung auf der Grundlage des Telekommunikationsgesetzes (fortan: Entwurf TKG-DSVO) wie folgt Stellung:

Eingangs sei in Kürze darauf hingewiesen, dass der Konsultation zur TKG-DSVO mehrere Besprechungsrunden des Fachverbandes der Telekommunikations- und Rundfunkunternehmungen unter der Leitung des Ludwig Boltzmann Instituts für Menschenrechte (BIM) vorausgegangen sind, wobei davor das BIM im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT) die Studie zur „Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung" ausgearbeitet hatte.

Wir begrüßen besonders, dass mit dem Anhang „Technische Richtlinie zur CSV-Datei für die Beantwortung von Auskunftsbegehren gemäß § 94 Abs 4 TKG 2003 - EP020", die auf Anregung unseres Fachverbandes der Telekommunikations- und Rundfunkunternehmungen erarbeitete Richtlinie EP 020 übernommen wurde.

Darüber hinaus erscheinen uns im Einzelnen die folgenden Überlegungen wesentlich:

1. Restriktive Möglichkeit für die mündliche Übermittlung von Anordnungen

Der letzte Absatz der erläuternden Bemerkungen zu § 3 Abs 2 DSVO ist zu streichen, da für Überwachungsmaßnahmen durch Anbieter nach der StPO grundsätzlich keine mündlichen Anordnungen vorgesehen sind (siehe § 138 StPO, in dem die sog Betreiberanordnung geregelt ist). Mündliche Anordnungen müssen auf die im Gesetz explizit genannten Ausnahmefälle beschränkt bleiben.
Eine Ausweitung auf StPO-Abfragen, wie in den EB zu § 3 Abs 2 DSVO festgehalten, ist aus Gründen der Rechtssicherheit abzulehnen. Eine derartige mündliche Anfrage auf Vorratsdaten in dringenden Fällen würde darüber hinaus dazu führen, dass die Anbieter für diese Datenanfragen einen Journaldienst (24/7) einführen müssten, was einerseits mit einem erheblichen

Aufwand und hohen Kosten verbunden wäre und anderseits dem TKG-Regelungsregime (insb § 102b Abs 2 TKG und EB zur RV) widersprechen würde. Die EB zur RV zum TKG idgF weisen ausdrücklich darauf hin, dass Anbieter zur Einrichtung eines Journaldienstes zur Erteilung von Auskünften über Vorratsdaten nicht verpflichtet sind.

2. Protokollierung

Gemäß § 7 Abs 3 Z 5 DSVO umfasst die Protokollierung auch die Speicherdauer der übermittelten Daten ab dem Datum, seit sie als Betriebsdaten und als Vorratsdaten gespeichert wurden. Diese Protokollierung geht auf Artikel 10 der Vorratsdatenspeicherungsrichtlinie zurück, der jedoch nur die Dauer, seitdem die Daten als Vorratsdaten gespeichert wurden, vorsieht. Zu den Betriebsdaten gibt es keine Bestimmung; eine solche ist auch nicht erforderlich. Daher erscheint es zweckmäßig, die entsprechende Bestimmung aus § 7 Abs 3 Z 5 DSVO zu streichen.

3. Auftraggeber und Dienstleister der Durchlaufstelle

Die Übermittlung der Daten erfolgt über eine zentrale Durchlaufstelle (kurz: DLS). Dafür sind Auftraggeber und Dienstleister sowohl zivilrechtlich als auch nach Datenschutzgesetz zu bestimmen. Auftraggeber sind aus datenschutzrechtlicher Sicht die Anbieter bzw die Behörden, für deren Anwendung Daten an die Durchlaufstelle übergeben oder von der Durchlaufstelle übernommen werden. Nach wie vor offen ist die Frage, ob eine Erklärung nach § 10 Datenschutzgesetz von den Anbietern übermittelt werden muss. Eine Haftung der Anbieter für Datenschutzverletzungen bei der DLS sollte (sofern sie grundsätzlich besteht) ausdrücklich ausgeschlossen werden, zumal die Anbieter die DLS nicht betreiben und auch nicht das Datensicherheitsniveau in der DLS beeinflussen können.

4. Verschlüsselung, Fortgeschrittene elektronische Signatur

Gemäß § 8 Abs 4 DSVO ist für die Identifizierung und Authentifizierung der Teilnehmer des Datenaustausches über die Durchlaufstelle eine fortgeschrittene elektronische Signatur erforderlich. Derzeit ist das Bundesrechenzentrum kein Anbieter einer solchen Signatur, was sich allerdings wohl ändern sollte.

5. Auditierung der Software

Nach § 8 Abs 3 DSVO müssen asymmetrische Verschlüsselungsverfahren als hybride Verfahren implementiert werden können. Dies erhöht zwar die Übertragungssicherheit, es ist aber ein erhöhter Aufwand für die Versendung des csv-Files zu erwarten, da ein bis zwei zusätzliche Arbeitsschritte für die Generierung eines eigenen "Session-Keys" und eines zusätzlichen Übertragungsfiles erforderlich sind. Zwei Schritte bei der Datenübermittlungen sind erforderlich, da einerseits das mit dem Session-Key verschlüsselte csv-File und andererseits der mittels Public-Key verschlüsselte Session-Key selbst übermittelt werden müssen. Genaueres kann jedoch erst nach Vorliegen der DLS-Spezifikationen gesagt werden. Daneben ist noch offen, welche Algorithmen für die Erzeugung eines Session-Key erforderlich sind - mit der Folge allfälliger Implementierungs- und Lizenzkosten.
Gemäß § 11 Z 3 DSVO darf nur eine auditierte schnittstellenkonforme Software für eine Datenübertragung verwendet werden. Streng genommen müssten dann auch Web-Services auditiert werden. Diese Bestimmung wird jedoch so ausgelegt, dass nur Client Software, die für diesen Zweck entwickelt wurde, zu auditieren ist. Provider Systeme fallen nicht darunter.

6. Unique ID

§ 17 Abs 2 DSVO enthält Bestimmungen für sogenannte Initialantworten. Das sind Antworten, zu denen es, zB als Folge einer mündlichen Anfrage, keine vorhergehende Anfrage über die DLS gibt. In solchen Fällen ist dem Grundgedanken der automatischen Unique-ID-Vergabe durch die DLS (wie auch in § 13 Abs 1 DSVO angeführt) zu entsprechen, indem von der DLS vollautomatisch eine Unique-ID vergeben wird und hier keinesfalls die Betreiber für die Vergabe dieser ID Sorge zu tragen haben. So könnte die Formulierung in § 17 Abs 2 DSVO dahingehend geändert werden, dass ein Bereich von Referenzen definiert wird, die von der Durchlaufstelle automatisch zu vergeben sind. Dieser Bereich muss nicht anbieterspezifisch sein und diese ID muss auch nicht vom Anbieter vergeben werden.

7. Optionale Stammdatenauskünfte

Nach § 21 DSVO können Anbieter und zugangsberechtigte Behörde im Einvernehmen optieren, Stammdatenauskünfte über die Durchlaufstelle abzuwickeln. Streng genommen würde dies eine Matrix von Vereinbarungen bedeuten. Gemeint ist hier, dass es einzelnen Betreibern freisteht, die optionalen Stammdatenauskünfte über die Durchlaufstelle anzubieten.

8. Protokollierung

Die Protokollierung nach § 23 Abs 2 DSVO erfordert, dass für die Erstellung der Statistik Informationen erforderlich sind, die auch Daten aus der staatsanwaltlichen Anordnung inkludiert. Ziel sollte eine möglichst weitgehend automatisierte Erfassung dieser Daten durch die Durchlaufstelle sein.

9. Investitionskosten

§ 24 DSVO bestimmt, dass auch die Investitionskosten für die Durchlaufstelle Investitionskosten gemäß § 94 Abs 2 TKG sind. Auch künftige Kosten (Upgrade, Release) sollten durch die Investitionskostenabgeltung inkludiert sein sollen. Weiters wäre klarzustellen, dass auch Eigenleistungen investitionskostenersatzfähig sind. Dies war auch bei der Implementierung im Jahr 2004 der Fall. Neben den unmittelbar anfallenden Investitionskosten bei Umsetzung der gegenständlichen TKG und DSVO Bestimmungen sollten auch künftige Investitionskosten für neue Dienste, die von der VDS betroffen sind, abgegolten werden.

Wir ersuchen um Berücksichtigung unserer Überlegungen und verbleiben

mit freundlichen Grüßen

Dr. Rosemarie Schön
Abteilungsleiterin