

An das
Bundesministerium für Verkehr,
Innovation und Technologie

Per Mail:
christian.singer@bmvit.gv.at

Betrifft: Entwurf einer Verordnung des Bundesministers für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO)
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 209. Sitzung am 3. Oktober 2011 **einstimmig beschlossen**, zu dem vorliegenden Verordnungsentwurf nachstehende Stellungnahme abzugeben:

Einleitend verweist der **Datenschutzrat auf** seine in der 206. Sitzung am 28. März 2011 **einstimmig beschlossene** Stellungnahme, zu den Regierungsvorlagen, mit denen die Vorratsdatenspeicherung umgesetzt wurde. Schon damals wurde betont, dass im Falle einer Umsetzung des Konzepts der Vorratsdatenspeicherung aus Sicht des Datenschutzes besonderes **Augenmerk auf den Aspekt der Datensicherheit gelegt werden sollte**. Der Datenschutzrat anerkannte, dass im TKG-Entwurf bereits diesbezügliche Regelungen vorhanden seien. Gleichwohl unterstrich er die vom deutschen Bundesverfassungsgericht in seinem Urteil vom 2. März 2010 zur Vorratsdatenspeicherung zum Thema der Datensicherheit getroffenen

Feststellungen. Demnach bedürfe es – aus Sicht des deutschen Bundesverfassungsgerichts - angesichts des **„Umfanges und der potentiellen Aussagekraft“** der als **Vorratsdaten zu speichernden Informationen eines „besonders hohen Sicherheitsstandards, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht“**. Diese grundsätzlichen Feststellungen sollen auch für Österreich gelten.

Allgemeines:

In das Telekommunikationsgesetz 2003 (TKG 2003) wurden anlässlich der jüngsten Novelle ausdrückliche Verordnungsermächtigungen aufgenommen, mit denen der Bundesminister für Verkehr, Innovation und Technologie ermächtigt wird, nähere Bestimmungen festzulegen, die der technischen Umsetzung der sog. Vorratsdatenspeicherung dienen. Es geht dabei um eine einheitliche Definition der Syntax, der Datenfelder und der Verschlüsselung, die Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung bestimmter Protokolle (vgl. § 94 Abs. 4 leg. cit.). Weiters ist im Verordnungswege eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit vorgesehen (§ 102c leg. cit.) Auch die Aufgaben und die Funktionsweise der der Implementierung der Protokollierungspflichten dienenden sog. Durchlaufstelle (DLS) sollen im Verordnungsweg festgelegt werden. Die DLS als solche ist nicht im TKG selbst angesprochen, sondern als technisches Mittel der Umsetzung der Protokollierungspflichten zu interpretieren.

Die inhaltliche Grundlage der nun vorliegenden Verordnung, welche die vorgenannten Regelungsziele erfüllen soll, bildet die Studie zur „Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung“, welche das Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des BMVIT ausgearbeitet hat, sowie die Diskussionen der insgesamt 6 Round Table Veranstaltungen des BIM im ersten Halbjahr 2011 zur Entwicklung der Schnittstellenbeschreibung und eines sicheren Systems der Datenübermittlung.

Datenschutzrechtlich relevante Bestimmungen:

Zu § 1:

In Abs. 2 sollte der letzte Halbsatz im Sinne einer harmonisierten Textierung (vgl. § 2 Abs. 1 Einleitungssatz) lauten: „soweit diese in Verbindung mit den zuvor genannten Datenkategorien verarbeitet werden.“

Zu § 2:

Im Sinne einer knapperen und zugleich leichter fasslichen Textierung sollte Abs. 1 Einleitungssatz lauten: „Verkehrsdaten, Zugangsdaten und Standortdaten sowie mit diesen Datenkategorien jeweils gemeinsam verarbeitete Stammdaten werden bezeichnet als [...]“.

In Abs. 1 Z 2 sollte wegen Redundanz das Wort „vorrätig“ entfallen oder stattdessen das Wort „gespeichert“ durch „gehalten“ ersetzt werden.

Zu § 3:

Es wird darauf hingewiesen, dass die Strafprozessordnung 1975 zuletzt mit BGBl. I Nr. 67/2011 geändert wurde.

Zu § 5:

In der Formulierung „betriebliche Rechtfertigung zur Speicherung als Betriebsdaten“ erscheint der Begriff „betriebliche“ mit Blick auf den spezifischen Gehalt des Begriffs „Betriebsdaten“ wiederum als redundant und daher verzichtbar.

Weiters wird in Abs. 3 in Abgrenzung zur „Vorratsdatenbank“ der Begriffe „betriebliche Datenbanken“ verwendet. Während Erstere in § 2 Abs. 2 Z 2 des Entwurfs definiert ist, fehlt es an einer vergleichbaren Legaldefinition für Letztere. Analoges gilt für den Passus „betrieblichen Speicherung“. Da diesen Begriffen offenbar spezifische Inhalte zugeschrieben werden, wird vorgeschlagen, eine entsprechende Ergänzung in § 2 leg. cit. vorzusehen. Anstelle „betrieblicher Speicherung“ könnte es im Übrigen auch heißen „Speicherung als Betriebsdaten“. Alternativ zur angesprochenen Ergänzung der Legaldefinitionen käme auch eine

Umformulierung in der Weise in Frage, dass mit den bereits jetzt in § 2 Abs. 1 und 2 leg. cit. definierten Begriffen das Auslangen gefunden wird.

Zu § 6 Abs. 1:

Zu Abs. 1 wird darauf hingewiesen, dass § 135 Abs. 2a der Strafprozeßordnung 1975 noch nicht in Kraft getreten ist (Gleiches gilt für § 19 Abs. 1, in dem auch auf § 135 Abs. 2a sowie auf § 76a der Strafprozeßordnung 1975 verwiesen wird). Es sollte durch Normierung einer Legisvakanz sichergestellt werden, dass nicht auf Bestimmungen verwiesen wird, die noch nicht in Kraft getreten sind.

Zu § 6 Abs. 3 fällt auf, dass wiederum als zusätzlicher Terminus Technicus jener der „betrieblich notwendigen Datenbanken“ eingeführt wird. Hier ist auf die Ausführungen zu § 5 zu verweisen und bietet sich eine entsprechende Harmonisierung der Normtexte an.

Zu § 9:

Der Datenschutzrat regt dringend an in Abs. 2 näher darzulegen, auf welche Bestimmung des Datenschutzgesetzes 2000 verwiesen wird.

Zu § 10 Abs. 2 Satz 2:

Da die Durchlaufstelle (DLS) stets Daten von Auftraggebern übermittelt bekommt (sei es als „Anfrage“ oder als „Antwort“) und diese entsprechend an den Empfänger weiterreicht, erscheint die Formulierung „für dessen Anwendung Daten an die Durchlaufstelle übergeben oder von der Durchlaufstelle übernommen werden“ insofern unzutreffend, als statt dem „oder“ ein „und“ zu setzen wäre.

Zu § 11:

Z 1 sieht vor, dass die Umsetzung der Durchlaufstelle „den Spezifikationen zur Durchlaufstelle“ zu entsprechen hat. Es ist unklar, ob damit die in der Anlage genannten „Technischen Richtlinien zur CSV-Datei (...)“ gemeint sind. Falls nicht sollte zum Ausdruck kommen, in welcher Weise diese Spezifikationen festgelegt werden.

Zu § 12:

In Abs. 6 sollte wohl auf „§ 22“ statt auf „§ 23“ verwiesen werden.

Zu § 13:

Abs. 3 enthält einen Verweis auf eine bestimmte Sicherheitsklasse der Portalverbundvereinbarung. Zur Wahrung des Publizitätsgrundsatzes sollte dargelegt werden, wo diese in der hier maßgeblichen Fassung publiziert worden bzw. einsehbar ist. Gleiches gilt sinngemäß für die Verweise auf die Portalverbundvereinbarung in § 16 Abs. 1 bzw. auf die Kommunikation Bürger – Behörde im Bereich E-Government in § 16 Abs. 2.

Zu § 19:

Der Datenschutzrat hält fest, dass die Kennzeichnung der Auskunftsbegehren nach ihrer Rechtsgrundlage in Bezug auf das SPG teilweise unzureichend ist. So umfasst § 53 Abs. 3a SPG idF ab 1 April 2010 neben dem Zugriff auf Internetprotokolladressen bzw. damit in Verbindung setzbare Identitätsdaten (vgl. Z 2 und 3 leg. cit.) auch den Fall der Ermittlung einer Telefonnummer eines Anrufers im Rahmen der Sprachtelefonie (vgl. Z 4 leg. cit.). Der Datenschutzrat bemerkt weiters, dass die fehlende Differenzierung in der Dokumentation nach § 19 die Überprüfbarkeit der Rechtmäßigkeit im Einzelfall beeinträchtigen könnte.

Zu § 22:

Hier fällt auf, dass in Abs. 1 davon die Rede ist, dass die Protokollierung der Durchlaufstelle (DLS) „keine personenbezogenen Daten“ enthält. Diese Aussage ist allerdings in dieser Form unzutreffend, wie zu zeigen sein wird. Analoges gilt für den 2. Satz des Abs. 1, der festhält, dass „[d]urch die Unique-ID jeder Anfrage [...] der Zusammenhang zwischen jeder Anfrage und deren Beantwortung ohne Personenbezug hergestellt“ wird. Gemäß § 13 Abs. 1 des Entwurfs vergibt die Durchlaufstelle zu jeder Anfrage eine einmalige, eindeutig zuordenbare Transaktionsnummer zur Prüfung der Authentizität der Anfrage und zur Nachverfolgung jeder Anfrage sowie deren Beantwortung (Unique-ID). Aus der Transaktionsnummer muss sowohl auf die zugrunde liegende konkrete Anfrage der

Behörde als auch auf den angefragten Betreiber geschlossen werden können. **Aus letzteren Aussagen ergibt sich, dass es sich bei den von der DLS protokollierten Daten jedenfalls insofern um personenbezogene handelt, als sie jeweils einer Behörde oder einem Betreiber, die ihrerseits als Grundrechtsträger in Betracht kommen, zugeordnet werden können. Und Letztere müssen die Daten anlässlich von datenschutzrechtlichen Überprüfungen wiederum mit konkreten Betroffenen in Bezug setzen können.**

Es wird weiters darauf hingewiesen, dass in den Erläuterungen von einem „Verweis auf § 7 Abs. 3 Z 3 bis 5“ die Rede ist: Im Unterschied dazu heißt es im Text des Verordnungsentwurfs „§ 7 Abs. 3 Z 4 und 5“ (vgl. Abs. 2).

Sollte – worauf zumindest die Erläuterungen zu § 22 hindeuten – die gesetzliche Deckung für Teile dieser Regelung fehlen, dann sollte eine Legisvakanz (bis zu einer Änderung der gesetzlichen Grundlage) vorgesehen werden.

Zu § 23:

Der Datenschutzrat bemerkt, dass in Bezug auf Abs. 3 praktisch kaum ein normativer Mehrwert im Vergleich zu § 102c Abs. 4 und 5 TKG 2003 besteht. Weiters wird normiert, dass „in der Spezifikation zur Durchlaufstelle ein elektronischer Zugang für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres vorzusehen [ist]“. **Ein Zugang für die Rechtsschutzbeauftragten ist als solcher nicht in § 102c TKG 2003 vorgesehen, somit fehlt es auch insofern an der gesetzlichen Deckung.**

Abschließend hält der Datenschutzrat fest, dass Änderungen und Ergänzungen im gegenständlichen Verordnungsentwurf sowie auch eine Änderung des Telekommunikationsgesetzes 2003 erforderlich sind.

4. Oktober 2011
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt