VERBAND ALTERNATIVER TELEKOM-NETZBETREIBER

Mariahilfer Straße 37-39, 5. OG
1060 Wien

jd@bmvit.gv.at

BMVIT, Sektion III, Abteilung PT 2,
Ghegastraße 1,
1030 Wien
Österreich

Datum: 13.Jannuar 2010
Bearbeiter: Mag. Florian Schnurer
Sekretariat: Claudia Pohl

Tel.: 01/588 39 DW 30
Fax: 01/586 69 71
E-Mail: schnurer@vat.at

DVR 0043257 ● ZVR 271669473

Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird - Geschäftszahl BMVIT-630.333/0001-III/PT2/2009 - Stellungnahme

Sehr geehrte Damen und Herren!

Der Verband Alternativer Telekom-Netzbetreiber nimmt zu dem gegenständlichen Entwurf wie folgt Stellung:

Grundsätzliches

Der Verband Alternativer Telekom-Netzbetreiber unterstützt eine sinnvolle Verbrechensbekämpfung und das Bestreben nach sachgerechten Lösungen zur grenzüberschreitenden Bekämpfung der organisierten Kriminalität und des Terrorismus. Allerdings müssen die Rahmenbedingungen für die Verbrechensbekämpfung verschiedenen Grundsätzen entsprechen.

Positiv an dem vorliegenden Entwurf ist hervorzuheben, dass die Einbindung der betroffenen Kreise im Zuge der Arbeit des Ludwig Boltzmann Instituts für Menschenrechte (BIM) bei der Erstellung eines Vorschlags für die Umsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG vorbildlich war. Das Institut hat diese komplexe Materie mit den betroffenen Kreisen diskutiert und so Lösungsansätze für die zahlreichen technischen und juristischen Probleme gefunden, die im Zuge der Umsetzung der Richtlinie identifiziert wurden.

An dieser Stelle muss darauf hingewiesen werden, dass der nun konsultierte Entwurf ein Gesamtgefüge von Regelungen in einem grundrechtssensiblen Rechtsgebiet beinhaltet, das durch zusätzliche punktuelle Änderungen des TKG 2003 (über die vorgeschlagenen hinaus) seine Ausgewogenheit verlieren würde. Der Entwurf berücksichtigt in sensibler Weise sowohl die Belange der Sicherheitsbehörden als auch die der betroffenen Unternehmen und ihrer Kunden. Mit dem Entwurf werden einerseits den Sicherheitsbehörden Ermittlungs- und Abwehrmöglichkeiten unter Verwendung von Verkehrsdaten ermöglicht und dies andererseits unter geringstmöglicher Eingriffsintensität in die Grund- und Menschenrechte gestattet.

Zu den Bestimmungen im Detail

Zu § 90 Abs. 6 bis 8
Nunmehr wird mit Abs. 7 gesetzlich klargestellt, unter welchen Voraussetzungen zur Strafverfolgung und Gefahrenabwehr Stammdaten zu beauskunften sind. Die Schaffung einer eindeutigen Rechtsgrundlage für die Beauskunftung von Stammdaten für Verwaltungsbehörden als auch für Beauskunftungen nach den Bestimmungen der StPO wird begrüßt. Wesentlich ist in diesem Zusammenhang auch die Definition, dass von diesen Bestimmungen ausschließlich Stammdaten umfasst sind, deren Beauskunftung ohne Verarbeitung von Verkehrsdaten möglich ist.

In § 92 Abs. 3 Z 16 wird auch gesetzlich klargestellt, dass dynamische IP-Adressen Verkehrsdaten sind, wie es der VfGH (Erkenntnis GZ 31/08 vom 1. Juli 2009), OGH (GZ 4 Ob 41/09x) und EuGH (Beschluss C-557/07 vom 19.2.2009) bereits - anders als der Strafsenat des OGH im Jahr 2005 (11 Os 57/05z) – wiederholt klargestellt haben. Durch diese gesetzliche Klarstellung werden Rechtsunsicherheiten und Judikaturdivergenzen in Bezug auf die Rechtsgrundlagen zur Beauskunftung dieser Datenkategorien beseitigt.

Zu § 93 Abs. 3
Der vorletzte Satz in den Erläuterungen *(„Für die Fälle einer nach der StPO zulässigerweise eingerichteten Fangschaltung bleibt die damit verbundene…“*) ist insofern nicht korrekt, da Auswertungen nach der StPO keine Fangschaltungen darstellen. Eine Fangschaltung darf lediglich nach § 106 TKG eingerichtet werden. Aus diesem Grund regen wir die Änderung der Wortfolge „*der StPO*“ in „*dem TKG*“ an.

Zu § 94 Abs. 1 und 2
Bereits im Vorblatt wird darauf hingewiesen, dass die Höhe der mit der Umsetzung der Richtlinie verbundenen Kosten nicht vorhersehbar ist. Die Höhe der Kosten hängt letztendlich vom Umfang der normierten Verpflichtungen ab und sind diese Mehrkosten in ihrer Gesamtheit derzeit nicht abschätzbar. Grundsätzlich entstehen den betroffenen Unternehmen Aufwände und Kosten aus der Speicherverpflichtung von verschiedenen, teilweise neu definierten Datenkategorien und der gegebenenfalls notwendigen „anderen Strukturierung“ der Speicherung von Vorratsdaten sowie weiters durch den erforderlichen erweiterten Speicherbedarf und die Schaffung einer Schnittstelle zur Beauskunftung.

Aufgrund des Erkenntnis des Verfassungsgerichtshofes (GZ 37/02-16 vom 27.02.2003), worin die den Ersatz von Investitionskosten ausschließende Bestimmung des § 89 Abs. 1 TKG 1997 als verfassungswidrig aufgehoben wurde, fordern wir eine klare gesetzliche Regelung zur Tragung der gesamten Kosten (Investitions- und Betriebskosten) durch die öffentliche Hand. Im Falle der Vorratsdatenspeicherung folgt die Speicherung allein im Interesse der Strafverfolgung, Betreiberinteressen sind nicht ersichtlich, weshalb ein Ersatz der Gesamtkosten aus unserer Sicht angemessen ist.

Hierzu muss im Zuge der Umsetzung der Vorratsdatenspeicherung auch die Anpassung der Überwachungskostenverordnung (ÜKVO) vorgenommen werden, um einen reibungslosen Ersatz für die Mitwirkung der Unternehmen bei der Überwachung zu gewährleisten. Diese Anpassung ist erforderlich, da durch die Vorratsdatenspeicherung neue Datenkategorien beauskunftet werden müssen (E-Mail Verkehrsdaten, Internetdaten, erweiterte Telefoniedaten) für die derzeit in der bestehenden ÜKVO keine Regelungen in Bezug auf die Höhe des Kostenersatzes vorgesehen sind.
Hinsichtlich einer Regelung in Bezug auf den Ersatz der Investitionskosten (§ 94 Abs. 1) ist es erforderlich, entweder die bestehende Investitionskostenverordung (IKVO) anzupassen oder eine eigenständige Verordnung zu erlassen, da sich die derzeit gültige

Investitionskostenverordnung (IKVO) ausschließlich auf Kosten bezieht, die dem Betreiber aus der Umsetzung der Überwachungsverordnung (ÜVO), BGBl. II Nr. 418/2001, entstanden sind. Zu erfassen sind neben den Kosten der Erstinvestition in die Technik auch Re-Investitionen im Rahmen von Erneuerungen und die Kosten für die Bearbeitung von Abfragen und auch weitere Kosten verursacht durch die auf Vorratsdaten bezogene Sicherungs- und Protokollierungspflichten.

Zur Schaffung größtmöglicher Rechtssicherheit ist daher eine zeitgleiche Anpassung der ÜKVO und der IKVO bzw. der Erlass einer Verordnung zum Ersatz der in Umsetzung der Richtlinie entstehenden Investitionskosten unumgänglich.

Zu § 94 Abs. 4
Im Rahmen der Diskussion mit dem BIM wurde deutlich, dass es neben einer Novelle des TKG 2003 weiterer Schritte bedarf, um die novellierten Bestimmungen des Telekommunikationsgesetzes praxisgerecht anwenden zu können. Ein ganz wesentlicher Punkt dabei ist die Definition einer Datenschnittstelle einschließlich eines Datenformats zur Übergabe der Vorratsdaten an die Behörden. Nur wenn dabei die Parameter eindeutig und verbindlich festgelegt sind, kann ein reibungsloser und somit schneller Datenaustausch zwischen den Unternehmen und den zuständigen Behörden gewährleistet werden.

Der Fachverband der Telekommunikations- und Rundfunkunternehmungen hat daher unter Einbeziehung der Telekommunikationswirtschaft begonnen, einen von der gesamten Branche mitgetragenen Vorschlag für eine technische Richtlinie auf Basis des im Entwurf vorgesehenen § 94 Abs. 4 TKG zu erarbeiten. Die Arbeiten an dieser Richtlinie werden zurzeit im Arbeitskreis für technische Koordination für öffentliche Kommunikationsnetze und -dienste (AK-TK) fortgeführt. Mit dieser Richtlinie kann der Verordnungsgeber auf eine Schnittstellendefinition zurückgreifen, welche die unterschiedlichen Kommunikationsarten berücksichtigt und ein Format nutzt, das auf Seiten der Behörden und der Betreiber einfach und ohne aufwändige Implementierungsmaßnahmen verarbeitet werden kann. Die Richtlinie wird voraussichtlich Ende Jänner 2010 fertiggestellt.

Der VAT begrüßt die Wahl des Formats CSV. Dieses Format ist kostengünstig umzusetzen und trägt damit zu einer möglichst gering belastenden Einführung der Vorratsdatenspeicherung in Österreich bei. Außerdem sprechen technische Aspekte für die Einführung dieses Formats. So befasst sich die Auskunft über Vorratsdaten mit Listen von Datensätzen. Das CSV-Format wurde gerade für die Verarbeitung von Listen von Datensätzen geschaffen und passt deshalb ideal für diesen Zweck. Ganz wesentlich ist der Vorteil, dass gängige Tabellenverarbeitungsprogramme (Excel, Open Office etc.) in der Lage sind, CSV-Daten zu ex- bzw. importieren. Jeder mit der Materie befasster Sachbearbeiter kann solche CSV-Dateien ohne Programmierkenntnisse erstellen oder weiterbearbeiten. Schließlich sind CSV-Dateien direkt lesbar und gestatten auch dem Sachbearbeiter eine leichte Verifikation, ob die richtigen Daten beauskunftet werden.
Im Rahmen der Diskussionen mit dem BIM wurde auch der ETSI-Standard (mit XML) evaluiert. Gegenüber dem CSV-Format hat er aus unserer Sicht folgende Nachteile: eine Schnittstelle zum Exportieren und Importieren dieser Daten ins XML-Format müsste für jede Auskunftsart programmiert werden, dies sowohl beim Betreiber als auch beim Empfänger. XML ist eine komplexe Datenstruktur, die die Repräsentation von komplexen Datenstrukturen ermöglichen soll. Vorratsdaten sind jedoch simple Datenstrukturen in Form einfacher Listen mit gleichbleibenden Spalten (z.B. Rufnummer, gerufener Nummer, Datum, Uhrzeit, Dauer der Verbindung etc.), für deren Verarbeitung dieses Format viel zu komplex wäre. Weiters ist XML in der Direktansicht viel schwieriger lesbar als CSV, zumal die eigentlichen Daten von jeder Menge Metazeichen (Tags) umhüllt sind. Die Zeilenstruktur eines Verkehrsdatums geht in der XML Ansicht verloren. Mit hoher Wahrscheinlichkeit

werden die beauskunfteten Daten beim Empfänger wieder mit Tabellenverarbeitungsprogrammen bearbeitet und ausgewertet. Dafür ist das Datenaustauschformat CSV am besten geeignet.

Die Verwendung des ETSI Standards wäre mit enormen und unverhältnismäßigen Kosten verbunden. Dies gilt sowohl auf Betreiberseite als auch auf Behördenseite.

Zusammenfassend ist festzuhalten, dass die bald finalisierte Technische Richtlinie ein sorgsam erörtertes und von der Telekommunikationswirtschaft getragenes Resultat der Bemühung um eine reibungslose Umsetzung der Vorratsdatenspeicherung in Österreich darstellt, das wir nachdrücklich als Basis für eine Verordnung gemäß dem vorgeschlagenen § 94 Abs. 4 TKG empfehlen.

Allerdings weisen wir darauf hin, dass diese Bestimmung in dieser Form in Zusammenhang mit Auskünften über aktuelle Standortdaten an Notrufträger, der Übermittlung von Ergebnissen von Online-Lokalisierungen (Peilungen außerhalb geführter Gespräche) zu laufenden Telefonüberwachungen oder auch bei laufenden Standortlokalisierungen aufgrund staatsanwaltschaftlicher Anordnungen äußerst problematisch ist, zumal in diesen Fällen eine telefonische Beauskunftung geboten ist. Darüber hinaus ist anzumerken, dass derzeit nicht jede Notrufstelle mit den entsprechenden technischen Einrichtungen zur Decodierung der codierten und verschlüsselten Daten ausgestattet ist.

Die in den Erläuterungen angeführte zusätzliche Verschlüsselung der Datenbanken beim Betreiber mittels Public Key der Behörden würde aus unserer Sicht auch Nachteile mit sich bringen und wird daher abgelehnt. Auch in den Erläuterungen wird dazu ausgeführt: "*Zu bedenken ist, dass in diesem Zusammenhang noch wesentliche Fragen der Umsetzbarkeit zu untersuchen sind, nicht zuletzt weil es hierfür einer entsprechenden staatlichen Infrastruktur bedarf. Eine Einbindung der Anbieter ist zur Definition einer solchen Verschlüsselungsvariante jedenfalls unabdingbar.*"

Da bei den betroffenen Unternehmen ohnedies entsprechende Sicherheitsvorkehrungen zum Schutz der Daten bestehen, wird dieser Vorschlag kritisch gesehen, da dies unter anderem auch zu einem massiven Eingriff in die gesamte Struktur der (individuellen) Datenhaltung der Unternehmen führen würde. Die Thematik sollte daher nach dem Ende der Begutachtungsfrist eingehend mit der Branche diskutiert werden.

Zu § 98 Abs. 2
In § 98 Abs. 2 wird vorgeschrieben, dass der Anbieter „*spätestens mit Ablauf der Rechnungsperiode*“ den Teilnehmer über die erfolgte Erteilung einer Auskunft (Standortlokalisierung) an Notrufträger zu informieren hat.

Fraglich ist in diesem Fall, wann die Benachrichtigung bei vorbezahlten anonymen Diensten (prepaid-Diensten) erfolgen soll, da in diesem Fall keine Rechnungsperiode (im Sinne einer monatlichen Rechnungsperiode) besteht.

Aus diesem Grunde und um Rechtsunsicherheiten zu vermeiden und einer möglichen Haftung von Anbietern bei Zweckvereitelung durch eine zu früh getätigte Information entgegenzuwirken sollte ein genau definierter Zeitraum, in dem der Anbieter seiner Informationspflicht nachkommen muss festgelegt werden.

Zu § 99 Abs. 1 und 2
Wir weisen ausdrücklich auf die durch die Ersetzung des Wortes „gesetzlich“ durch die Wortfolge „in diesem Gesetz“ erfolgte Klarstellung hin: Die rechtliche Zulässigkeit und die Speicherungszwecke von Verkehrsdaten sind im TKG abschließend geregelt. Auch dass aus

materiellen Auskunftsansprüchen in anderen Materiengesetzen keine implizite Berechtigung oder gar Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann (war schon bisher herrschende Ansicht), erfährt damit eine Klarstellung.

Zu den Erläuterungen Besonderer Teil zu § 99 Abs. 1 und 2
Wir erlauben uns, die Korrektur eines Redaktionsfehlers vorzuschlagen: § 99 Abs. 1 und 2 müsste richtigerweise „Abs. 1 und 4“ lauten.

Zu § 99 Abs. 5 Z 1
Hier erfolgt im Interesse der Strafverfolgung eine wichtige gesetzliche Klarstellung, mit der nunmehr im TKG explizit die Beauskunftung in Fällen sog. niederschwelliger Straftaten (mit Strafdrohungen unterhalb derer von Straftaten, für deren Verfolgung auf Vorratsdaten zugegriffen werden darf) geregelt wird und - dogmatisch korrekt - auf § 134 StPO ff verwiesen wird. Allfälliger Kritik daran, dass gemäß § 134 StPO ff ein Strafmindestmaß erforderlich ist, kann nicht im Rahmen von § 99 des Entwurfs begegnet werden. Dies wäre allein im Wege einer Änderung der Strafprozessordnung zu ändern.

Zu § 99 Abs. 5 Z 2
Wir weisen hierzu auf die fundierten Erläuterungen zum Begutachtungsentwurf hin, dass Verkehrsdaten vom Schutz des Fernmeldegeheimnisses gemäß Art. 10a StGG erfasst sind, weshalb eine Auskunft über Verkehrsdaten ausschließlich aufgrund einer richterlichen Genehmigung erfolgen darf. Dieser Grundsatz wird hier für jene Fälle durchbrochen, in denen die Auskunft für die Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen notwendig ist.

§ 99 Abs. 5 Z 1 und 2 beruhen auf intensiven Diskussionen mit der Branche und zeigen, dass den Bedürfnisse der Sicherheits- und Strafermittlungsbehörden Rechnung getragen wurde. Diese Bestimmungen sind ein praktikabler Vorschlag, wie künftig die bisher zulässige Beauskunftungspraxis im Sinne aller Beteiligten fortgeführt werden kann.

Allerdings wird darauf hingewiesen, dass die Anforderungsvoraussetzungen des ersten Satzes („…, wenn diese Auskunft als wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen notwendig ist.“) nicht mit jenem der §§ 53 Abs. 3a und 3b SPG im Einklang stehen. Das heißt, dass - wie in der Erläuterung zu §§ 99 Abs. 5 Z 2 richtig festgehalten – für die Sicherheitspolizei zwar der Zugriff auf alle Daten, die schon bisher zulässigerweise bei den Anbietern vorhanden waren, grundsätzlich bestehen bleibt, jedoch aufgrund der einschränkenderen Voraussetzungen des TKG - trotz Anforderung nach §§ 53 Abs. 3a oder 3b SPG – die Auskunft nicht erteilt werden darf, da die gesetzliche Auskunftsermächtigung ausdrücklich auf diesen (einschränkenderen) TKG-Absatz verweisen muss. Es wird daher angeregt, die Anforderungsvoraussetzungen des SPG und TKG aufeinander abzustimmen.
Betreffend die Festlegung jenes Zeitraumes innerhalb dessen der Anbieter nach dieser Bestimmung seiner Informationspflicht nachzukommen hat, verweisen wir auf unsere Ausführungen zu § 98 Abs 2.

Zu § 102a Abs. 1
Die Ausführungen in den Erläuterungen zur Speicherdauer und die Minimalumsetzung einer sechsmonatigen Speicherung von Vorratsdaten sind zu begrüßen. Eine darüber hinausgehende Speicherdauer würde für die Betreiber erhebliche Kosten und Aufwand verursachen. Ebenso wäre eine darüber hinausgehende längere Speicherdauer für eine verdachtsunabhängige Datenspeicherung ein unverhältnismäßiger Grundrechtseingriff für die davon Betroffenen.

§ 102a Abs. 2 Z 1

Die erläuternden Bemerkungen zu der im Gesetzesentwurf geregelten Speicherverpflichtung für Anbieter von Internetzugangsdiensten (§ 102 a Abs. 2) regeln hinsichtlich der Speicherpflicht von IP-Adressen, dass sich diese im Sinne der Richtlinie nur ausschließlich auf Accessprovider zugewiesene öffentliche IP Adressen bezieht. Interne Adressen und IP-Ports (z.B. entstanden durch NAT gemäß RFC 1631, RFC 2663, RFC 3022) sind nach den Erläuterungen nicht von der Speicherverpflichtung umfasst.

Klarstellend sollte dazu festgehalten werden, dass diese Regelung sowohl interne IP-Adressen betrifft, die einem Teilnehmer von einem Provider zugewiesen wurden, als auch jene internen IP-Adressen betrifft, die ein Teilnehmer hinter einer von einem Betreiber zugewiesenen öffentlichen IP-Adresse verwendet. Insoweit ein Provider Teilnehmern interne IP-Adressen zugewiesen hat, wäre es für den Provider im Falle eines Auskunftsbegehrens auf Vorratsdaten (NAT Adressen) unverhältnismäßig eine große Anzahl von möglichen Nutzerdaten von (an einer Straftat) Nichtbeteiligten zu beauskunften.

Zum besseren Verständnis halten wir fest, dass verschiedenste NAT/PAT Vorgänge einer großen Anzahl von Teilnehmern zum gleichen Zeitpunkt ein und dieselbe öffentliche IP-Adresse zugewiesen wird, mit der sie im Internet in Erscheinung treten – Rückschlüsse auf einzelne Teilnehmer sind daher nicht möglich. Eine weite Auslegung der Beauskunftungspflicht würde einer grundrechtskonformen Umsetzung der Vorratsdatenspeicherungsrichtlinie widersprechen, und überdies keine für die Strafverfolgung verwertbaren Daten liefern. Es ist daher insbesondere in den erläuternden Bemerkungen zu § 102 Abs 2 Z 1 klarzustellen, dass Anbietern von Internetzugängen bei der Verwendung von NAT Adressen keine Verpflichtung zur Beauskunftung sämtlicher zu dieser öffentlichen IP-Adresse möglichen Teilnehmer trifft.

Zu § 102a Abs. 3 Z 6 lit c

Gemäß § 102 a Abs. 3 Z 6 lit c) TKG-Entwurf obliegt Betreibern von Mobilfunknetzen zudem unter anderem die Speicherung der Kennung des Standortes (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt. Wir weisen darauf hin, dass eine Umsetzung dieser Verpflichtung für die Betreiber mit hohem technischen Aufwand und Kosten verbunden ist.

Zu § 102a Abs. 4 Z 1 und 2

Wir weisen in diesem Zusammenhang darauf hin, dass die Funktionalität der Historisierung von E-Mail Adresszuordnungen (inkl. Alias) systembedingt in den verwendeten Anlagen nicht verfügbar ist. Nur bei aktuellem Empfang oder Versand wird eine (gegebenenfalls nur temporär) zugewiesene E-Mail Adresse dazu verwendet eine Zustellung in das korrekte Postfach zu gewährleisten. Im Wesentlichen bedeutet dies, dass zwar Verkehrsdaten zu einer (gegebenenfalls auch temporär) zugewiesenen E-Mail Adresse zwar gespeichert und ausgewertet werden können, eine Zuordnung zu einem Teilnehmer jedoch nur dann möglich ist, wenn die E-Mail Adresse aktuell noch gültig ist.

Zu § 102a Abs. 8

Hier wäre in Satz 1 ein redaktionelles Versehen zu korrigieren und hinter zu löschen "oder zu anonymisieren" analog § 99 Abs. 1 anzufügen.

Zu § 102b Abs. 1

Dass Auskünfte über Vorratsdaten nur zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten erteilt werden dürfen, ergibt sich aus der zugrundeliegenden Richtlinie und wäre auch ohnedies aufgrund der Intensität des Grundrechtseingriffs zwingend

geboten, um den Grundsatz der Verhältnismäßigkeit zu wahren. Damit ist gleichzeitig geklärt, dass Vorratsdaten nicht für die Verfolgung von Urheberrechtsverletzungen zur Verfügung stehen. Hierzu gibt es andere Daten (siehe § 99 Abs. 5 Z 1 des Entwurfs).

Eine Auskunft über Vorratsdaten darf gemäß § 102b nur aufgrund einer gerichtlichen Bewilligung und zum Zwecke der Ermittlung, Feststellung und Verfolgung schwerer Straftaten an die nach StPO zuständigen Behörden erfolgen. Derzeit ist für die betroffenen Unternehmen unklar, was unter der Definition "*schwere Straftat*" zu verstehen ist, die in den bezugnehmenden Gesetzen, die Auskunftsbegehren regeln, aufzunehmen ist. Diesbezüglich fordern wir, dass eine Beauskunftung nur bei Verbrechen gemäß § 17 Abs. 1 StGB und Offizialdelikten erfolgen soll.

Zu § 102c Abs. 2 Z 5
Wir regen die Streichung von Z 5 an, da – zumindest für den Anbieter – oft der Name und die Anschrift des von der Beauskunftung betroffenen Teilnehmers nicht bekannt (z.B. anonyme Wertkarte, Strafsache gegen unbekannten Täter etc.) und somit nicht protokollierbar sind. Weiters ist eine Auswertung der Stammdaten nur für Teilnehmer im eigenen Netz möglich.

Des Weiteren ist unklar, ob sich die Protokollierungspflicht des Anbieters aufgrund dieser Ziffer auch auf jene Teilnehmer, welche von der überwachten Teilnehmernummer kontaktiert wurden oder diese kontaktiert haben (d.h. Teilnehmer, welche aufgrund bzw. im Zuge der Auswertung ermittelt werden), erstreckt, da sich der Gesetzeswortlaut und die Erläuterungen (letzter Satz zu § 102c Abs. 2 Z 5) in diesem Punkt widersprechen. Von einer extensiven Auslegung dieser Ziffer – so wie in den Erläuterungen beschrieben, d.h. von einer (automatischen) Erhebung bzw. Protokollierung von Stammdaten sämtlicher aufgrund einer Auswertung ermittelten Teilnehmer – ist aufgrund der nicht bewältigbaren Datenmenge abzuraten. Insbesondere auch deswegen, da diese Teilnehmer nicht direkt die von der Auskunft über Vorratsdaten betroffenen Teilnehmer darstellen und diese überschießende Informationen somit nicht dem Zweck dieser Bestimmung dienen.

Zu § 102c Abs. 3
Um einer laufenden Protokolldatenübermittlung vorzubeugen, regen wir folgende Ergänzung bzw. Änderung der Ziffern an:
Z 1 die Protokolldaten gemäß Abs. 2 auf schriftliches Ersuchen *jährlich bis zum 31.1. für das vorangegangene Kalenderjahr* der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission;
Z 2 die Protokolldaten gemäß Abs. 2 Z 1 bis 4 auf schriftliches Ersuchen *jährlich bis zum 31.1. für das vorangegangene Kalenderjahr* dem Bundesministerium für Justiz.

In den Erläuterungen zu dem Gesetzesentwurf sollte auch klarstellend festgehalten werden wann die Protokolldaten spätestens zu löschen sind.

Zu den im Entwurf festgelegten aufwendigen Protokollierungspflichten ist derzeit auch kein Kostenersatz vorgesehen. Aufgrund des für Betreiber verbundenen hohen Aufwandes bei Erfüllung von Protokollierungspflichten, ist zumindest ein angemessener Kostenersatz vorzusehen.

Zu § 109 Abs. 3 Z 22
Wir begrüßen, dass diese Bestimmung Straffreiheit vorsieht, sofern die notwendigen Investitionskosten noch nicht aufgrund einer nach § 94 Abs. 1 erlassenen Verordnung abgegolten wurden.

Fehlen einer Übergangsbestimmung
Der Entwurf enthält derzeit keine Fristen für eine technische Umsetzung der normierten Verpflichtungen durch die Betreiber. Aufgrund des hohen technischen Aufwandes bei den Betreibern bedarf es jedenfalls der Festlegung angemessener Umsetzungsfristen. Daher fordern wir die gesetzliche Festlegung einer angemessenen, zumindest neunmonatigen Übergangsfrist, um österreichweit eine einheitliche Umsetzung zu gewährleisten.

Wir weisen darauf hin, dass umfangreiche technische Implementierungsmaßnahmen notwendig sind, die sinnvollerweise erst dann begonnen werden können, wenn der Umfang der Speicherverpflichtung endgültig feststeht (d.h. ab Inkrafttreten des Gesetzes), da andernfalls erhebliche Investitionen umsonst getätigt worden sein könnten. Es ist weiters zu berücksichtigen, dass nach technischer Umsetzung (Datenbank, Systeme und Schnittstellen) die entsprechende Datenbank erst sukzessive aufgebaut werden kann, da die von der Vorratsdatenspeicherung umfassten Daten derzeit bei den Betreibern nicht gespeichert werden.

Wir ersuchen um Berücksichtigung unserer Stellungnahme.

Mit freundlichen Grüßen

VAT – VERBAND ALTERNATIVER TELEKOM-NETZBETREIBER

Mag. Florian Schnurer, LL.M.