An das
Bundesministerium für Verkehr,
Innovation und Transport
III/PT2 (Recht)
Ghegastraße 1
1030 Wien
JD@bmvit.gv.at

Kopie an:
begutachtungsverfahren@parlament.gv.at

Wien, am 21. Mai 2007

Betreff: ***BMVIT-630.333/0001-III/PT2/2007*** **– Novelle des TKG 2003, Umsetzung der Richtlinie über die Vorratsdatenspeicherung**

Sehr geehrte Damen und Herren,

die ISPA, der Verband der österreichischen Internetanbieter, nimmt zum Entwurf der Novelle des TKG 2003, mit der die Richtlinie 2006/24/EG („Data Retention Richtlinie“) umgesetzt wird, wie folgt Stellung:

Der Eingriff in die Grundrechte muss so gering wie möglich gehalten werden

Die verdachtsunabhängige Speicherung von Kommunikationsdaten aller Bürger stellt einen massiven Grundrechtseingriff dar. Die Richtlinie rechtfertigt diesen Eingriff damit, dass die Daten ausschließlich zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten, insbesondere von Terrorismus und organisierter Kriminalität verwendet werden dürfen. Die ISPA hat mehrfach[1] darauf hingewiesen, dass dies insbesondere im Hinblick auf Art 8 der Europäischen Menschenrechtskonvention (EMRK), der den Schutz des Privat- und Familienlebens gewährleisten soll, aufgrund der Schwere des Eingriff nicht ausreichend ist. Umso mehr ist darauf zu achten, dass die Grundrechtseingriffe so gering wie möglich gehalten werden, insbesondere, indem an die Schwere der Straftat hohe Anforderungen gestellt werden und der Zugriff auf die Daten *nur aufgrund eines schriftlichen Beschlusses eines Strafrichters* erfolgen darf. Aus Sicht der ISPA entspricht die Gleichsetzung der “schweren Straftat“ mit dem Begriff der „mit beträchtlicher Strafe bedrohten Handlung“ des § 17

[1] zuletzt im Positionspapier zur verdachtsunabhängigen Speicherung von Verkehrs- und Standortdaten (Data Retention) http://www.ispa.at/downloads/positionspapier_dataretention.pdf.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

SPG dieser Anforderung in keiner Weise, da von dieser Definition sogar Fahrlässigkeitsdelikte (!) umfasst sind. Aus Sicht der ISPA muss der Zugriff auf die Daten auf *Verbrechen (§ 17 Abs. 1 StGB; vorsätzliche Handlungen, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind)*, soweit sie Offizialdelikte sind, beschränkt sein. Darüber hinaus müssen Regelungen in anderen Gesetzen (etwa § 87b Abs 3 UrhG, § 53 Abs 3a SPG) so angepasst werden, dass unmissverständlich klar ist, dass die Vorratsdaten *nur im Strafverfahren auf schriftlichen richterlichen Beschluss* und nicht etwa im Verwaltungsverfahren oder gar in zivilrechtlichen Angelegenheiten verwertet werden dürfen. Nur durch die Entscheidung eines Richters kann sichergestellt werden, dass der Eingriff in das Grundrecht auf Datenschutz sowie in Art 8 EMRK gerechtfertigt ist und der Betreiber nicht allfälligen Schadenersatzansprüchen der Betroffenen ausgesetzt ist.

Klarheit und Rechtssicherheit darüber, was zu speichern ist

Die ISPA begrüßt, dass die österreichische Umsetzung der Date Retention Richtlinie die niedrigstmögliche Speicherdauer von 6 Monate vorsieht. Um Unklarheiten zu vermeiden, ist klarzustellen, dass die Daten 6 Monate ab dem Zeitpunkt der Beendigung des Kommunikationsvorgangs gespeichert werden müssen.

Problematisch ist die im Entwurf vorgesehen Neufassung des Begriffs „Stammdaten“. Diese ist aus Sicht der ISPA nicht notwendig, da die bisherige Fassung mit der Data Retention Richtlinie im Einklang steht. Gänzlich abzulehnen ist die vorgesehene Vermischung von Verkehrs- und Vorratsdaten (Verweis auf Daten „gemäß Z 4a lit a“ in § 92 Abs 3 Z 3 lit a), da sie inhaltlich unrichtig und darüber hinaus verwirrend ist. Insbesondere würde die Formulierung den Zugriff auf bestimmte Arten von Vorratsdaten *ohne* die Vorraussetzungen des § 149a StPO iVm § 102a TKG 2003 in der Fassung des Entwurfs erlauben, was jedenfalls vermieden werden muss.

Speicherung von Internetdaten

Österreich hat die Möglichkeit gemäß Art 15 Abs 3 der Richtlinie in Anspruch genommen, die Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail bis zum 15. März 2009 aufzuschieben. Die Ausnützung dieser Frist ist aus Sicht der ISPA jedenfalls notwendig, um die technischen und wirtschaftlichen Folgen einer Speicherung dieser Daten evaluieren zu können und eine verhältnismäßige Implementierung zu ermöglichen.

Die Entwurf sieht einige neue Begriffe vor, die insbesondere im Hinblick auf das Internet zu Unklarheiten führen. In § 92 Abs 3 Z 2a wird unter die Definition von Telefondienst auch E-Mail subsumiert. Die ISPA fordert die Streichung dieser Definition, da sie im Bezug auf E-Mail zu Widersprüchen führt und im übrigen die allgemeines Definition des Telefondiensts ausreichend ist. Die Definition der Benutzerkennung in § 92 Abs 3 Z 2b ist unklar. Es handelt sich dabei wohl im wesentlichen um eine Kundennummer, die als Stammdatum sowieso gespeichert wird. Daher ist auch diese Definition entbehrlich und kann gestrichen werden.

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Wenn die erläuternden Bemerkungen die Einführung eines Teils der Maßnahmen im Zusammenhang mit dem Internet schon mit der vorliegenden Novelle damit begründen, dass Rechtssicherheit im Zusammenhang mit der Beauskunftung von IP-Adressen durch Internet Service Provider geschaffen würde, ist dem in zweierlei Hinsicht zu widersprechen: Einerseits würde es zu diesem Zweck jedenfalls ausreichen, diejenigen Daten gemäß § 92 Abs 4a lit a sublit bb (richtig wohl: § 92 Abs 3 Z 4a lit a sublit bb) zu speichern, die den Internetzugang betreffen. Daher wäre die Wortfolge „Internet-E-Mail und Internet-Zugang“ zu streichen, da die relevanten Daten zur Beauskunftung einer IP-Adresse nur beim Zugangs-(Access-)Provider vorhanden sind. Andererseits ist die Rechtsnatur der IP-Adresse durch den vorliegenden Entwurf keineswegs geklärt. Es müsste zu diesem Zweck ausdrücklich klargestellt werden, dass es sich bei der IP-Adresse um ein Verkehrsdatum im Sinne des § 92 Abs 3 Z 4 handelt und dass diese sowie ihre Verknüpfung mit den Stammdaten (insbesondere über den Zeitpunkt der Zuordnung der IP-Adresse zu einem bestimmten Endgerät) daher nur (als Ausnahme zu § 99) im Rahmen der Data Retention gespeichert und gemäß § 149a StPO iVm § 102a TKG 2003 in der Fassung des Entwurfs an das Strafgericht beauskunftet werden darf.

Die Daten gemäß § 92 Abs 3 Z 4a lit e sublit cc und lit f betreffen ihrem Inhalt nach nur die Mobiltelefonie und sind, um Missverständnisse zu vermeiden, unter § 92 Abs 3 Z 4a lit. e sublit. bb einzuordnen.

Kostenersatz

Im Vorblatt zum Gesetzesentwurf wird festgehalten, dass die vorgesehene Speicherverpflichtung „ausschließlich Daten betrifft, die bereits derzeit für Verrechnungszwecke gespeichert werden.“ Dies ist jedenfalls im Bezug auf Daten, die das Internet betreffen, unzutreffend: Tatsächlich müssten Daten gespeichert werden, die derzeit noch nicht gespeichert werden. Weiters fallen Investitionskosten, etwa für sichere Systeme bzw. Schnittstellen, an. Die Höhe dieser Kosten ist, wie auch aus den Erläuterungen zum Entwurf hervorgeht, noch nicht abschätzbar.

Darüber hinaus sieht das Gesetz Verpflichtungen für Anbieter und Betreiber öffentlicher Kommunikationsnetze vor, die deren Kosten der Vorratsdatenspeicherung unnötigerweise erhöhen. Die Pflicht zur Protokollierung von Zugriffen und Übermittlungen durch Betreiber gemäß § 102a Abs 4 sowie die Auskunftspflichten gemäß § 102b sind nicht notwendig. Diese Informationen müssen ja auch bei den Gerichten vorhanden sein, sodass für die Anbieter und Betreiber ein ungerechtfertigter Zusatzaufwand entstehen würde. Da auch die RL 2006/24/EG nicht vorsieht, dass die Protokollierungs- und Informationsverpflichtungen gerade den Anbietern und Betreibern auferlegt werden müssen, sollten diese gestrichen werden.

§ 102a Abs 3 gibt lediglich Art 7 lit a-c der RL 2006/24/EG wieder. Inhaltlich ist die Regelung unklar und der allfällige Implementierungsaufwand nicht abschätzbar. Aus Sicht der ISPA sind in § 14 DSG 2000 schon ausreichende Maßnahmen im

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

Zusammenhang mit Datenschutz und Datensicherheit vorgesehen, sodass § 102a Abs 3 entfallen sollte.

Bei der Vorratsdatenspeicherung handelt es sich um eine Maßnahme, die ausschließlich der Strafverfolgung, also zur Erfüllung einer staatlichen Aufgabe dient. Die zu speichernden Daten haben für die Betreiber keinerlei wirtschaftlichen Wert. Den Betreibern sind daher sowohl die laufenden als auch die Einrichtungskosten der Speicherung und Bereitstellung der Daten zeitnahe mit der technischen Umsetzung zu ersetzen. Der Ersatz der Investitionskosten könnte auch in Form einer steuerlichen Absetzbarkeit der Investitionen oder der Einrichtung eines Fonds ausgestaltet werden.

In diesem Zusammenhang sei auch auf das Erkenntnis des VfGH vom 27.2.2003 (G 37/02 ua) verwiesen, wonach zur Kostenabgeltung an Betreiber hinsichtlich der Telekommunikationsüberwachung der Verhältnismäßigkeitsgrundsatz zu beachten ist.

Wir ersuchen, dass unsere Anregungen berücksichtigt werden.

Mit freundlichen Grüßen,

Roland Türke
Präsident

Kurt Einzinger
Generalsekretär

address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977