An das
BMVIT, Sektion III, Abteilung PT 2
Ghegastraße 1, 1030 Wien

per E-Mail jd@bmvit.gv.at

GZ: BMVIT-630.333/0001-III/PT2/2009

Wien, am 15. Jänner 2010

Betreff: Entwurf für eine Novelle des Telekommunikationsgesetzes zur Umsetzung der „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG"

Sehr geehrte Damen und Herren,

Die ISPA, als Vertreter der Internetwirtschaft, möchte die vorgegebene Frist bis 15.01.2010 nutzen, um zum vorliegenden Entwurf des oben genannten Gesetzesvorhabens nachstehende Stellungnahme abzugeben.

Wir begrüßen ausdrücklich die mit einem Zeitraum von acht Wochen angesetzte längere Begutachtungsfrist, da es sich um ein Thema handelt, das nicht nur für die betroffene Branche, sondern für die gesamte Zivilgesellschaft grundlegende Auswirkungen nach sich ziehen wird.

1. Kritikpunkte an der Richtlinie

1.1. Beste Umsetzung der Data Retention – RL ist sie nicht umzusetzen

Die „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG" (Data Retention RL, im folgenden kurz „Richtlinie“) bietet einen umfassenden Paradigmenwechsel im Europäischen Datenschutzniveau. War bisher die Löschung von nicht mehr zweckmäßig gespeicherten Daten oberste Maxime des durch die Datenschutz-Richtlinie (RL 2002/58/EG) geformten

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

Rechtsrahmens, sieht die Richtlinie eine verdachtsunabhängige Speicherung einer erheblichen Anzahl von (zumindest teilweise sensiblen) Kommunikationsdaten für eine Dauer von mindestens sechs bis maximal 24 Monaten vor.

Der Hintergrund und die Entstehungsgeschichte der Richtlinie aus dem Jahr 2006 ist in den Terroranschlägen in London und Madrid mit dem Ziel zu finden, durch die Speicherung von Kommunikationsdaten einen harmonisierten Datenpool zur Abwehr und Aufklärung schwerer Straftaten, insbesondere Terrorismus, zu schaffen. Konkret sollen Verbindungsdaten, im Wesentlichen wer, mit wem, wann, wie lange, von wo aus und über welchen Dienst (E-Mail, SMS, Mobil- und Festnetztelefonie, Internettelefonie, Internet) kommuniziert hat, nicht aber die Inhalte, für einen Zeitraum zwischen mindestens sechs Monaten und maximal zwei Jahren verpflichtend gespeichert werden.

Nach der aktuellen österreichischen Rechtslage dürfen Verbindungsdaten nur für Verrechnungszwecke bis zum Ablauf jener Frist gespeichert werden, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann (vgl § 99 TKG 2003). Dies entspricht in der Praxis (je nach Betreiber AGB) regelmäßig einem Zeitraum zwischen drei und sechs Monaten. Nach unseren Erfahrungen ist diese aktuelle rechtliche Situation für die Aufklärung und Verfolgung von Straftaten ausreichend und es besteht unserer Ansicht nach kein Bedarf an einer zusätzlichen verdachtsunabhängigen Speicherung zur Unterstützung der Aufklärung und Verfolgung von Straftaten. Den Betreibern ist es ein großes Anliegen, die Aufklärung und Verfolgung von Straftaten zu unterstützen. Auf der anderen Seite muss auch dafür Verständnis aufgebracht werden, dass die Betreiber als Erbringer von Dienstleistungen gegenüber ihren Kunden gewisse Schutz- und Sorgfaltspflichten zu erfüllen haben, auf ein klares rechtliches Umfeld angewiesen sind und für einen fairen Ausgleich der Interessen der Kunden auf Privatheit und des Staates auf Erfüllung seiner Aufgaben einstehen. Der Ansatz einer zusätzlichen verdachtsunabhängigen Speicherung von Daten, die im Regelbetrieb zu Verrechnungszwecken in der nun gewünschten Form regelmäßig nicht anfallen würden, und deren Fehlen auch bisher einer erfolgreichen Aufklärung oder Verfolgung von Straftaten nicht entgegengewirkt hat, ist daher aus unserer Sicht als überschießende Maßnahme im Sinne der Verhältnismäßigkeit und aus grundrechtlichen Überlegungen abzulehnen. Da aus unserer Sicht eine verfassungskonforme Umsetzung der Richtlinie nicht möglich ist, regen wir an konsequenterweise die Richtlinie nicht umzusetzen.

1.2. Keine Klärung offener Fragen durch zurückgezogenen Entwurf 2007

Mit der vorliegenden Novelle sollen Betreiber von Telekommunikationsdiensten dazu verpflichtet werden Verkehrs- und Standortdaten, die beim Erbringen von Kommunikationsdiensten erzeugt oder verarbeitet werden für Zwecke der Strafverfolgung zu speichern. Bereits im Jahr 2007 wurde ein entsprechender Gesetzesentwurf zur Begutachtung versendet, der auf umfassende Ablehnung und ernsthaften Widerstand der betroffenen Kreise gestoßen ist (vgl dazu ua die ISPA Stellungnahme, abrufbar unter http://www.ispa.at/stellungnahmen/novelle-des-tkg-2003-umsetzung-der-richtlinie-ueber-die-

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

vorratsdatenspeicherung/). Die Hauptkritikpunkte am damaligen Entwurf waren mangelnde grundrechtliche Abwägungen, unklare Begriffsbestimmungen (Gegenstand und konkrete Dauer der Speicherpflichten) damit einhergehend fehlende Rechtssicherheit sowie unzureichende Feststellungen betreffend Kostenersatz.

2. Externe Beauftragung und Einbeziehung der betroffenen Kreise bei der Umsetzung schaffen einen in sich geschlossenen und abgewogenen Gesamtkompromiss

2.1. Orientierung an Mindestumsetzung und strenge Sicherungsmaßnahmen zum Schutz der Grundrechte

Im Gegensatz zum Umsetzungsentwurf aus dem Jahr 2007 wurde bei den Vorarbeiten zum vorliegenden Entwurf erkannt und festgehalten, dass es sich um eine Speicherung von Daten auf Vorrat ohne Verdachtsmomente gegen eine bestimmte Person handelt und damit höchste datenschutzrechtliche und rechtsstaatliche Standards einzuhalten sind (siehe Begleitschreiben zur Veröffentlichung des Entwurfs v 20.11.2009). Konsequenterweise schlägt der vorliegende Entwurf eine Mindestumsetzung der EU-Richtlinie mit maximal sechsmonatiger Speicherdauer der Daten, die Verwendung nur für die Aufklärung von schweren Straftaten und nur mit gerichtlicher Anordnung (Ausnahme drohende Gefahr für Gesundheit oder Leben) vor. Weiters wird eine strenge Verwendungskontrolle der Daten (umfassende Dokumentations- und Informationspflicht) festgeschrieben und der zu speicherende Datenumfang auf die konkreten Forderungen der Richtlinie beschränkt. Durch strikte Regelungen zur Speicherung und Übergabe der Daten und weiterer Kontrolle durch die unabhängige Datenschutzkommission sind wichtige Parameter für einen effizienten Missbrauchsschutz festgelegt, die durch die im Entwurf vorgesehene Zugriffsprotokollierung und der Verpflichtung zur verschlüsselten Übermittlung verstärkt werden. Nach Ansicht der ISPA ist eine Orientierung an den Mindestanforderungen der Richtlinie vollkommen ausreichend und zu unterstützen. Besonderes Augenmerk muss darauf gelegt werden, dass die inhärenten Ziele der Richtlinie, Aufklärung von schweren Straftaten und Verhinderung von Terrorismus, verfolgt werden und keine Ausweitung des Anwendungsbereichs auf Bagatellfälle oder zivilrechtliche Streitigkeiten durchgeführt wird. Wir unterstützen weiter die vorgeschlagenen Sicherungsmaßnahmen, da jede Speicherung von Daten ein Missbrauchsrisiko in sich birgt, das es angemessen zu minimieren gilt. Die vorgeschlagenen Maßnahmen des beschränkten Zugangs, der Zugriffsprotokollierung, getrennten Verwendung, Kontrolle durch die unabhängige Datenschutzkommission und der verschlüsselten Übergabe stellen bereits erprobte und praktikable Maßnahmen zur Missbrauchskontrolle dar.

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

2.2. Einbeziehung einer Expertengruppe unter Federführung des Ludwig Boltzmann-Institut für Menschenrechte zum größtmöglichen Grundrechtsschutz

Das Ziel der Richtlinie, eine verdachtsunabhängige Speicherung von Kommunikationsdaten, kann nur mit grundrechtlichen Einschränkungen erreicht werden. Der vorliegende Entwurf einer externen Expertengruppe unter Federführung des Ludwig Boltzmann-Instituts für Menschenrechte (BIM) bietet nun ein ausgewogen balanciertes Bündel an Maßnahmen, um eine geringstmögliche Umsetzung der Richtlinie und größtmöglichen Schutz persönlicher Daten und Grundrechte zu erhalten. Vor diesem Hintergrund muss beachtet werden, dass auch nur kleine Änderungen oder Anpassungen in den Formulierungen große Auswirkungen auf das Gesamtsystem der geplanten Regelung nach sich ziehen würden und damit zu einer komplett anderen Einschätzung des Entwurfs führen würden. Wir anerkennen die Bemühungen der Expertengruppe als konstruktiv und grundrechtsschonend an und sehen in dieser vom Ministerium gewählten Vorgehensweise großes Potential auch für zukünftige Gesetzesvorhaben, die sich insbesondere im Spannungsverhältnis zwischen staatlichen Aufgaben und Grundrechten bewegen.

3. Weiterführung der intensiven Einbeziehung der betroffenen Kreise und Ausdehnung auf verwandte Materien zur Schaffung optimaler gesellschaftspolitischer und wirtschaftlicher Rahmenbedingungen

Nach den positiven Erfahrungen rund um die Einbeziehung der betroffenen Kreise in die Expertengruppe zur Erstellung eines Umsetzungsentwurfs, die in einem konstruktiven Prozess einen ausgewogenen Vorschlag erarbeiten konnten, regen wir zukünftig eine frühzeitige Einbeziehung sowie ein Weiterbeschreiten dieses sinnvollen konstruktiven Weges an. Die Gelegenheit ergibt sich schon konkret bei den Nachfolgearbeiten zum Entwurf, also bei den Verordnungen zum Kostenersatz und der Verordnung zur näheren Bestimmung zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsselung zur Übermittlung der Daten in einer technischen Richtlinie (vorgeschlagener § 94 Abs 4 TKG 2003). So hat die Branche im Rahmen des Arbeitskreises für Technische Koordination für öffentliche Kommunikationsnetze und -dienste (AK-TK) eine Arbeitsgruppe mit dem Titel „Schnittstellendefinition zur Vorratsdatenspeicherung“ (kurz „Schnittstellendefinition“) eingesetzt, die sich mit den offenen Fragen zu dem Thema aus dem Blickwinkel der Industrie beschäftigt und eine Empfehlung für das Thema „Schnittstellendefinition gemäß TKG § 94 (4)" erstellt. Diese Empfehlung wird von der ISPA unterstützt und beschreibt den von der Industrie im Rahmen des AK-TK abgestimmten Vorschlag für die Schnittstelle zur Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG und soll in Weiterführung einer positiven Zusammenarbeit eine Vorarbeit für die im Entwurf vorgeschlagene technische Richtlinie darstellen.

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

4. Speicherverpflichtung für die Dauer von sechs Monaten ist ausreichend

Die im Entwurf vorgesehene Speicherdauer von sechs Monaten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation (vorgeschlagener § 102a TKG 2003), entspricht einer Minimalumsetzung der Richtlinie und kann vor dem Prinzip der Verhältnismäßigkeit sowie dem Wunsch nach einer möglichst praxistauglichen Lösung nur Zustimmung finden. 95% der Anfragen von Ermittlungsbehörden beziehen sich auf Vorfälle, die weniger als 6 Monate zurückliegen. Die Speicherdauer darf daher keinesfalls länger als 6 Monate sein, um die Eingriffe in die Privatsphäre der Bürgerinnen und Bürger und deren Grundrecht auf Schutz ihrer personenbezogenen Daten so gering wie möglich zu halten.

5. Vernünftige Ausnahmemöglichkeit für kleine Providern von der Speicherpflicht

Bei kleinen Providern steht das Verhältnis der Investitionskosten bzw. Kosten des laufenden Betriebs sowie der organisatorische Aufwand zur Etablierung von sicheren Beauskunftungsprozessen in keiner Relation zur wahrscheinlich geringen Anfragehäufigkeit durch die Behörden. Nach der KMU Definition (KMU Definition vgl Empfehlung der EU Kommission 2003/361/EG: „kleine Unternehmen“) werden kleine Unternehmen definiert als Unternehmen, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanzsumme höchstens 10 Mio. EUR beträgt. Die ISPA unterstützt die im Entwurf (vorgeschlagener § 102a Abs 6 TKG 2003) enthaltene Regelung als eine sinnvolle und verhältnismäßige Regelung, die zB auch in Deutschland in ähnlicher Form umgesetzt wurde. Nach unserer Ansicht besteht in diesen Fällen auch kein Verfolgungsrisiko, da ein Zugriff – wie im bisher funktionierenden System – auf die aktuell gespeicherten Verrechnungsdaten auch bei ausgenommenen Betreibern weiter möglich ist.

6. Zugriff auf Vorratsdaten nur für die Verfolgung schwerer Straftaten und grundsätzlich nur unter richterlicher Kontrolle

Die Beauskunftung von Vorratsdaten sollte – wie auch Ziel der Richtlinie – nur zum Zwecke der Verfolgung von schweren Straftaten unter richterlicher Kontrolle erlaubt sein. Für die Beauskunftung sonstiger Straftaten ist eine ausdrückliche gesetzliche Regelung als datenschutzrechtliche Zweckbindung notwendig, um die aktuelle unsichere rechtliche Situation für alle Beteiligten zu klären. Diese Klärung soll einen raschen Zugriff bei Gefährdung von Leben oder Gesundheit eines Menschen, sonst unter richterlicher Kontrolle ermöglichen. Ausnahmen von einer richterlichen ex ante Kontrolle sind – wie im Entwurf vorgesehen – natürlich im Anwendungsbereich des Sicherheitspolizeigesetzes (SPG) zur Abwehr einer konkreten Gefahr für das Leben oder zum Schutz der Gesundheit eines Menschen notwendig (vgl den Fall der Ortung eins Vermissten oder eines Entführungsopfers anhand des Mobiltelefons). Zur Wahrung des Rechtsschutzniveaus regen wir in diesen „Akutfällen“ zumindest eine richterliche ex post Überprüfung für den jeweiligen Einzelfall an.

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

Eine nachträgliche Überprüfung durch den Rechtsschutzbeauftragten scheint uns nach den bisherigen Erfahrungen mit der Kontrolle der SPG Anfragen bei der Verwendung von Vorratsdaten als zu wenig weitgehend. Ansonsten sehen wir die im Entwurf vorgeschlagenen Regelungen betreffend Auskunft über Vorratsdaten (vorgeschlagener § 102b Abs 1 TKG 2003), die eben eine Auskunft nur aufgrund gerichtlicher Bewilligung vorsehen und einer ausdrücklichen verweisenden gesetzlichen Bestimmung bedürfen als sehr brauchbare Bestimmung zur Verwirklichung eines zweckgebundenen Zugriffs, der natürlich noch die entsprechenden Pendants in den entsprechenden Materiengesetzen (zB StPO) benötigt. In diesem Zusammenhang ist auch eine Klärung des Begriffs der „schweren Straftaten“ notwendig. Dieser in der österreichischen Rechtsordnung an sich undefinierte Begriff, der als Übersetzung aus der Richtline „serious crimes“ schwer wiegende Straftaten bezeichnet, lässt sich unserer Ansicht nach am ehesten mit der Unterteilung in Vergehen und Verbrechen (§ 17 StGB) auflösen, die Verbrechen als vorsätzliche Handlungen, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind, definiert und Fahrlässigkeitsdelikte, sowie "niederschwellige" Straftaten ausklammert. Für letztere besteht dann noch immer die Möglichkeit der Beauskunftung unter Zugriff auf die für betriebsnotwendige Zwecke gespeicherten Verkehrsdaten, wenn eine gerichtliche Bewilligung vorliegt (vgl, vorgeschlagener § 99 Ab. 5 Z 1 TKG 2003). Wir sehen mit den vorgeschlagenen Regelungen ein ausgewogenes System geschaffen, das je nach Schwere der Straftat und rechtsstaatlicher Kontrolle einen geordneten Zugriff auf die Daten zulässt.

7. „Collateral Benefit“ – Gesetzliche Bereinigung aktueller Graubereiche

Neben der Umsetzung der Richtlinie sieht der Entwurf sehr begrüßenswerte Klarstellungen und damit Bereinigungen gesetzlicher Graubereiche vor, die in ihrer Gesamtheit zu einer positiven Bewertung des Entwurfs führen. So wird im Entwurf nun ausdrücklich abschließend klargestellt, dass Verkehrsdaten außer in den im TKG geregelten Fällen weder gespeichert noch verwendet werden dürfen und vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren sind (vorgeschlagener § 99 TKG 2003), dies mit dem Ziel, Rechtssicherheit dahingehend zu schaffen, dass aus anderen gesetzlichen Bestimmungen weder eine Berechtigung noch eine Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann. Dies entspricht dem Fazit der Erkenntnisse des VfGH und des OGH aus dem Jahr 2009 und findet hier seine gesetzliche Klarstellung. Letztendlich auch aus diesen Erkenntnissen abgeleitet, fließt zutreffend die rechtliche Einordnung der IP-Adresse als Zugangsdatum und damit als Verkehrsdatum in den Entwurf ein. Durch diese Qualifizierung wird (zumindest die dynamische IP Adresse) durch das Fernmelde- wie auch des Kommunikationsgeheimnisses geschützt und ein langjährige Auslegungsfrage zwischen Betreibern und Behörden gesetzlich geklärt.

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

8. Voller Kostenersatz für die Erfüllung eines ausschließlich staatlichen Interesses

Bei der geplanten Vorratsdatenspeicherung werden Daten gespeichert, die für den Betreiber in dieser Form keinen wirtschaftlichen Wert aufweisen. Es handelt sich um eine Maßnahme, die ausschließlich der Aufklärung und Verfolgung von Straftaten, also der Erfüllung staatlicher Aufgabe dient. Den Betreibern sind daher sowohl die laufenden als auch die Einrichtungskosten der Speicherung und Bereitstellung der Daten sehr zeitnahe mit der technischen Umsetzung zu ersetzen. Weiters sind auch die zukünftigen notwendigen Kosten zu berücksichtigen. Die Investitionskostenverordnung (IKVO) sowie die Überwachungskostenverordnung (ÜKVO) sind entsprechend zu ergänzen, wobei ein Kostenersatz sich immer am tatsächlichen Aufwand zu orientieren hat. So müssen sich die Kosten für eine Beauskunftung jeweils an den einzelnen Kundenabfragen und nicht zB an einer Ereignisabfrage (an dem einmal mehr oder weniger Kunden beteiligt sind) orientieren, was auch den Vorteil eines grundrechtlichen Regulierungsinstruments durch die Kostentragung bieten würde. Wir sehen die klare Vorschreibung eines angemessenen Kostenersatzes durch Verordnung im Entwurf (§ 94 Abs 2 TKG 2003) sowie die Bezugnahme auf das Erkenntnis des Verfassungsgerichthofes hinsichtlich Kostenersatzes vom 27.2.2003, G 37/02-16 positiv und weisen ausdrücklich darauf hin, dass von Seiten der Betreiber kein wirtschaftliches Interesse an den Daten besteht und schon durch die Einrichtung und Umgestaltung der Systeme enorme Kosten auf die einzelnen Betreiber zukommen. Hier sind bei weitem höhere Kosten, insbesondere für den Betrieb zu erwarten, als zB durch die Einführung des ETSI Standards entstanden sind, die nicht mit einem Ersatz für die Investitionskosten abgegolten werden können. Wir fordern aus diesen Gründen eine Anpassung der entsprechenden Kostenersatzregelungen um einen vollen Kostenersatz für Initial- und laufende Kosten zu gewährleisten. Die entsprechenden Kostenersatzregelungen müssen parallel mit dem Gesetz in Kraft treten, um Verzögerungen beim Ausgleich und Ersatz der anfallenden Kosten (wie beim Erlass der IKVO) zu vermeiden.

9. Anpassungsbedarf: Datenübermittlung an Notrufträger

Abschließend sehen wir noch Anpassungsbedarf im Punkt Übermittlung der Nutzerinformation gegenüber Notrufträger (§ 98 Abs 2 TKG 2003). Bei Vorliegen eines Notfalls würde eine Übermittlung der Standortkennung (vgl vorgeschlagener § 98 Abs 2 TKG 2003) nach dem strengen Regime der Handhabung von Vorratsdaten (Übertragung auf geschütztem Weg per CSV Datei) einen zu starren, unflexiblen Prozess bedingen. Im Anwendungsbereich des § 98 TKG 2003 würden wir eine Ausnahme zur Beibehaltung der aktuellen Übermittlungform bei Notfällen anregen, um zB eine rasche Standortpeilung bei abgängigen Minderjährigen oder suizidgefährdeten Personen zu ermöglichen.

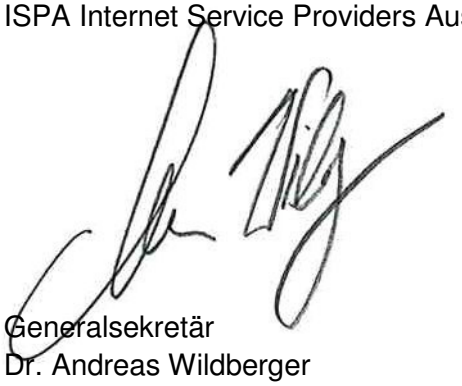
address: 1090 wien, währingerstraße 3/18 • austria • europe
phone: +43-1-4095576 • fax: +43-1-409557621 • mail: office@ispa.at • web: http://www.ispa.at • zvr:551223675
UID-Nr.: ATU 543 97 807 • IBAN=AT59 1200 0006 6049 1705 • BIC=BKAUATWW • blz:12000 • bank austria:00660491705 • dvr:0931977

10. Zusammenfassung

Die Data Retention RL stellt einen krassen Paradigmenwechsel im Europäischen Datenschutzniveau dar und ist unserer Ansicht nach nicht ohne Grundrechtstangierung umsetzbar. Der vorliegende, unter intensiver Einbeziehung von Industrie, BMI und BMJ unter Federführung des BIM erarbeitete, Entwurf regelt nicht nur die Umsetzung der Richtlinie, sondern bietet auch zusätzlich eine gesetzliche Bereinigung aktueller rechtlicher Graubereiche und stellt damit ein ausgewogenes Bündel von Maßnahmen für eine grundrechtsschonende Umsetzung dar.

Als Interessensvertretung der Internetwirtschaft in Österreich sehen wir in der Einbeziehung der betroffenen Kreise eine wichtige Entwicklung hin zu einem konstruktiven gesellschaftspolitischen Prozess und regen eine Weiterführung der intensiven Einbindung der betroffenen Kreise und Ausweitung auf andere Themen an.

Mit freundlichen Grüßen
ISPA Internet Service Providers Austria



Generalsekretär
Dr. Andreas Wildberger

Ergeht per E-Mail an:

- BMVIT, Sektion III, Abteilung PT 2

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