An das
Bundesministerium für Wissenschaft,
Forschung und Wirtschaft
ABTEILUNG C2/1
Stubenring 1
1010 Wien

E-Mail: not9834@bmwfw.gv.at

Wien, am 11. Februar 2015

BETREFF: ISPA-STELLUNGNAHME ZUM UK-ENTWURF EINES TERRORBEKÄMPFUNGS- UND SICHERHEITSGESETZES 2014 (*Counter Terrorism and Security Bill 2014)*, NOTIFIKATION NR.: 2014/576/UK

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, im Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Wissenschaft, Forschung und Wirtschaft im Rahmen des EG-Infoverfahrens betreffend den UK-Entwurf des Terrorbekämpfungs- und Sicherheitsgesetzes 2014 (*Counter Terrorism and Security Bill 2014)*, Notifikation Nr. 2014/576/UK, wie folgt Stellung zu nehmen.

Die ISPA vertritt die Ansicht, dass der Gesetzesentwurf geltendem europäischem Recht sowie der aktuellen Judikatur[1] des EuGH widerspricht, und ist der Meinung, dass dieser unverhältnismäßig in die Grundrechte auf Achtung des Privat- und Familienlebens sowie des Schutzes personenbezogener Daten eingreift.

Die ISPA weist drauf hin, dass angesichts der Aufhebung der Vorratsdatenrichtlinie durch den EuGH (C-293/12 und C-594/12) die Speicherung von *„relevant internet data“* einen wesentlich einschneidenderen Eingriff in die Grundrechte der Betroffenen darstellt und daher überdacht werden soll.

ISPA weist darauf hin, dass die gesetzliche Definition von *„relevant internet data“* ausgesprochen vage formuliert ist, was zu Rechtsunsicherheit bei den Betreibern führt. Sofern die Verpflichtung zur Speicherung von *„relevant internet data“* nicht zur Gänze aus dem Entwurf gestrichen wird, schlägt die ISPA als Lösungsvorschlag die Einführung einer abschließenden Aufzählung jener Daten, die unter die Kategorie *„relevant internet data“* fallen, vor. Ferner würde die ISPA eine ausdrückliche Klarstellung, dass die Verarbeitung von *„relevant internet data“* auf Dienste-Ebene

[1] EuGH, C293/12 und C-594/12, vom 8. April 2014

nicht vom Gesetzesentwurf umfasst ist und die Betreiber somit nicht zu einer Speicherung von Daten auf Dienste-Ebene verpflichtet werden dürfen, sehr begrüßen.

Die ISPA weist drauf hin, dass die für die Speicherung notwendige anlasslose und flächendeckende Anwendung der *„Deep Packet Inspection"* Technologie einen unzulässigen und unverhältnismäßigen Eingriff in den Datenverkehr und damit wohl in die Privatsphäre der Nutzerinnen und Nutzer darstellt und daher von den österreichischen Betreibern ausdrücklich abgelehnt wird.

Die ISPA lehnt jegliche Vorbildwirkung des britischen Gesetzesentwurfs auf künftige österreichische gesetzgeberische Akte ab.

1. Die Speicherung von *„relevant internet data"* stellt einen unverhältnismäßigen Eingriff in die Grundrechte der Betroffenen dar und soll neu überdacht werden.

Teil 3. des UK-Terrorbekämpfungs- und Sicherheitsgesetzes sieht eine Verschärfung der britischen Nachfolgeregelung der aufgehobenen Vorratsdatenspeicherungsrichtlinie - Data Retention and Investigatory Powers Act (DRIPA) - vor. Mit der vorliegenden Novelle sollen Betreiber von Telekommunikationsnetzen und -diensten dazu verpflichtet werden, neben Verkehrs-, Standort- und Betriebsdaten auch eine neue Kategorie von Daten, die sogenannten *„relevant internet data"*, die beim Erbringen von Kommunikationsdiensten erzeugt werden, zum Zwecke der Strafverfolgung zwölf Monate lang zu speichern.

Es handelt sich hierbei um Informationen, durch die eine öffentliche IP-Adresse mit der Identität einer Nutzerin oder eines Nutzers oder des verwendeten Geräts zu jedem gegebenen Zeitpunkt verknüpft werden kann.

Der Ansatz einer zusätzlichen verdachtsunabhängigen Speicherung von Daten, die im Regelbetrieb nicht durchgeführt würde, stellt aus unserer Sicht eine überschießende Maßnahme im Sinne der Verhältnismäßigkeit dar, da das von der Datenschutzrichtlinie 2002/52/EG verlangte angemessene Verhältnis der Maßnahme zum intendierten Zweck, nämlich eine Reduktion der Terrorgefahr, nicht sichergestellt ist. Darüber hinaus konnte bisher die Wirksamkeit jeglicher Vorratsdatenspeicherung für die erfolgreiche Verhinderung, Aufklärung oder Verfolgung von Straftaten nicht belegt werden, wodurch diese der datenschutzrechtlichen Anforderung „geeignet sein" nicht entspricht. Die Speicherung von *„relevant internet data"* widerspricht somit unserer Ansicht nach den Bestimmungen der Datenschutzrichtlinie 2002/52/EG und verkennt die aktuelle Rechtsprechung des EuGH[2], welche zur Aufhebung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG geführt hat.

Vor diesem Hintergrund hält die ISPA die Verpflichtung zur anlasslosen, flächendeckenden Speicherung von *„relevant internet data"* für einen unverhältnismäßigen Eingriff in die Grundrechte

[2] EuGH, C293/12 und C-594/12, vom 8. April 2014

auf Achtung des Privat- und Familienlebens sowie des Schutzes personenbezogener Daten der Betroffenen und regt deshalb an, diese Bestimmung aus dem Gesetzesentwurf zu streichen.

2. Die unscharfe Definition von *„relevant internet data“* führt zu Rechtsunsicherheit.

Die Bestimmung betreffend die *„relevant internet data“* ist unscharf formuliert und enthält keine konkreten oder abschließenden Angaben über jene Daten, die in diese Kategorie fallen könnten. In den gesetzlichen Erläuterungen (explanatory notes) sind lediglich exemplarisch einzelne Beispiele für *„relevant internet data“* wie MAC Adressen (Media Access Control) oder Portnummern genannt.

Der vage Wortlaut sowie die diesbezüglich unzureichenden Ausführungen in den Erläuterungen lassen die Frage ungeklärt, welche Daten die Datenkategorie *„relevant internet data“* umfasst. Die Beurteilung, ob ein Datum als *„relevant internet data“* zu kategorisieren ist und folglich der Vorratsdatenspeicherungspflicht unterliegt, ist zur Gänze den Betreibern von Telekommunikationsnetzen und -diensten überlassen.

Angesichts der mangelnden Erläuterungen in Bezug auf den Umfang der Speicherpflicht wären die Anbieter gezwungen eine möglichst umfangreiche Palette an Daten auf Vorrat zu speichern, um den gesetzlichen Anforderungen nachzukommen und allfällige Gesetzesverstöße zu vermeiden. Gleichzeitig haben die Betreiber als Erbringer von Dienstleistungen ihren Kunden gegenüber gewisse Schutz- und Sorgfaltspflichten zu erfüllen und sind deshalb auf ein klares rechtliches Umfeld angewiesen. Die Anbieter von Telekommunikationsnetzen und -diensten stehen für einen fairen Ausgleich der Interessen der Kunden an Privatsphäre und des Staates an der Erfüllung seiner Aufgaben ein.

Aufgrund der unscharfen Formulierungen ist weder ein fairer Interessenausgleich noch ein klares rechtliches Umfeld durch die gegenständliche Gesetzesnovelle sichergestellt. Diese würde zu erheblicher Rechtsunsicherheit führen und wird daher strikt abgelehnt.

Sofern die Verpflichtung zur Speicherung von *„relevant internet data“* nicht zur Gänze aus dem Entwurf gestrichen wird, regt die ISPA als Lösungsvorschlag im Sinne der Rechtssicherheit eine klare, abschließende Aufzählung jener Daten an, die unter der Kategorie *„relevant internet data“* fallen.

3. Eine Erstreckung der „*relevant internet data*“ auf Informationen der Dienste-Ebene würde zu einer anlasslosen, flächendeckenden inhaltlichen Analyse von Internet-Kommunikationsvorgängen führen.

Eine Speicherung von „*relevant internet data*“ setzt voraus, dass diese Daten für den Anbieter verfügbar sein müssen. Um die zu speichernden Daten verfügbar zu machen bzw. die erforderlichen Parameter zu identifizieren, hat eine laufende Überwachung sowie unter Umständen eine inhaltliche Analyse der Kommunikation zu erfolgen.

Eine extensive Interpretation des Terminus „*relevant internet data*“, welche die Speicherung von Informationen auch auf der Dienste-Ebene (z.B. Informationen über Skype-Kommunikationsvorgänge oder über VPN-Verbindungen) vorsähe, würde dazu führen, dass von den Betreibern eine Analyse des Inhaltes der Datenströme (sog. „*deep packet inspection*“) seiner Nutzerinnen und Nutzer durchgeführt werden müsste, um Daten über die gewünschten Kommunikationsvorgänge zu erhalten. Als deep packet inspection (DPI) wird ein Verfahren in der Netzwerktechnik bezeichnet bei der Datenpakete überwacht werden. Dabei werden gleichzeitig der Datenteil als auch der Headerteil des Datenpaketes nach deren Dekodierung einer Analyse unterzogen.

Diese ausgedehnte Auslegung würde nicht nur Betreiber von Telekommunikationsnetzen und -diensten treffen, sondern indirekt auch Anbieter von Diensten der Informationsgesellschaft, beispielweise Betreiber von Webseiten und Onlineshops. Für die Zuordnung einer öffentlichen IP-Adresse benötigt ein Netzbetreiber die interne IP-Adresse, die Portnummer und Login-Daten vom Webseitenanbieter, um die Identität des Webseitennutzers oder des verwendeten Geräts zum gegebenen Zeitpunkt feststellen zu können.

Die grundrechtliche Eingriffsintensität einer derartigen anlasslosen, flächendeckenden inhaltlichen Analyse der gesamten Kommunikation übertrifft daher jedenfalls die einer – ebenso anlasslosen sowie flächendeckenden und für unzulässig erklärten - Vorratsdatenspeicherung und ist aus diesem Grund strikt abzulehnen.

ISPA fordert daher eine ausdrückliche Klarstellung, dass die Verarbeitung von *„relevant internet data“* auf Dienste-Ebene jedenfalls nicht von der Regelung des Punktes 17 des UK-Terrorbekämpfungs- und Sicherheitsgesetzes umfasst ist und Betreiber somit weder zu einer Verarbeitung noch zu einer Speicherung von Daten auf Dienste-Ebene verpflichtet werden dürfen.

Die ISPA hoffte auf die Aufnahme und Weitergabe ihrer Bedenken und Anregungen.

Für Rückfragen (und weitere Auskünfte) stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

Die ISPA – Internet Service Providers Austria –ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von rund 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.