An das
Bundesministerium für Arbeit, Soziales und Konsumentenschutz
Stubenring 1,
A-1010 Wien

E-Mail: Alexandra.Hammerl@sozialministerium.at
iris.podbelsek-auer@sozialministerium.at
christian.palmetzhofer@sozialministerium.at

Wien, am 20. Oktober 2016

BETREFF: ISPA-STELLUNGNAHME ZUM VORSCHLAG DER EU-KOMMISSION ZUR ÄNDERUNG DER VERORDNUNG ÜBER DIE ZUSAMMENARBEIT ZWISCHEN DEN FÜR DIE DURCHSETZUNG DER VERBRAUCHERSCHUTZGESETZE ZUSTÄNDIGEN NATIONALEN BEHÖRDEN („REGULATION ON CONSUMER PROTECTION COOPERATION - CPC“)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich im Zusammenhang mit der Konsultation des Bundesministeriums für Arbeit, Soziales und Konsumentenschutz zum Vorschlag der EU-Kommission zur Änderung der Verordnung über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden („Regulation on consumer protection cooperation - CPC“) wie folgt Stellung zu nehmen:

Die ISPA weist zunächst darauf hin, dass die vorgesehenen Befugnisse einen unverhältnismäßigen Eingriff in Grundrechte darstellen und nicht der Rechtsprechung des Europäischen Gerichtshofs entsprechen. Ferner resultiert aus der Unbestimmtheit der Begrifflichkeiten des Verordnungsentwurfes erhebliche Rechtsunsicherheit. Die ISPA fordert, dass die Beauskunftung von Kundendaten jedenfalls nur gegen Kostenersatz und gemäß den strengen Formvorschriften des österreichischen Rechts zu erfolgen hat. Die ISPA betrachtet die Anordnung zur Umsetzung von Zugangssperren an Access-Provider generell als ungeeignete, drakonische sowie kostenintensive Maßnahmen welche abzulehnen sind. Zudem stellen Netzsperren kein effizientes Mittel dar, um Konsumenten vor allfälligen Bedrohungen wie „fake-shops“ und anderen Gefahren zu schützen und fordert die ISPA, dass der Begriff „Domain“ gänzlich aus Art. 8 gestrichen wird. Zudem weist die ISPA darauf hin, dass es in Österreich, aufgrund des weitreichenden Anwendungsbereichs der Richtlinie zu einer immensen Ausuferung sensibler Eingriffsbefugnisse käme und fordert, dass die datenschutzrechtlichen Bestimmungen bei der Weiterverwendung der gesammelten Daten beibehalten werden.

1. **Die vorgeschlagenen Befugnisse stellen einen unverhältnismäßigen Eingriff in Grundrechte dar und widersprechen der Judikatur des EuGH**

Der Entwurf der EU-Kommission sieht in Art 8. CPC gewisse Mindestbefugnisse für Konsumentenschutzbehörden zur Wahrnehmung ihrer Aufgaben vor. Die vorgeschlagenen Befugnisse greifen insbesondere in das Recht auf Datenschutz (Art. 8 GRC) ein, jedoch auch in einige andere Grundrechte wie zB. das Recht auf Privatleben (Art. 7 GRC) im Zusammenhang mit den Eingriffen in das Hausrecht und das Telekommunikationsgeheimnis. In den jeweiligen Bestimmungen in Art 8 CRC ist jedoch in keiner Weise eine Abwägung gemäß dem Verhältnismäßigkeitsgrundsatz vorgesehen. Auch ist keine gerichtliche Bewilligung einzelner Maßnahmen oder eine ex-post Kontrolle durch Gerichte vorgesehen. Vielmehr wird dies den Mitgliedsstaaten in Art. 9 Abs. 1 lit. a, b CPC vollkommen freigestellt.

Dies erinnert an die EU-Richtlinie zur Vorratsdatenspeicherung welche durch die Entscheidung des EuGH in der Rs Digital Rights (C-293/12) aufgehoben wurde. Die Richtlinie sah eine Verpflichtung für die Mitgliedstaaten vor, in das Recht auf Privatleben und das Recht auf Datenschutz einzugreifen indem Telekommunikationsbetreiber dazu verpflichtet wurden, äußere Daten der Telekommunikation auf Vorrat zu speichern. Der EuGH machte deutlich, dass ein derartiger Eingriff auch mit den notwendigen grundrechtlichen Absicherungen verbunden sein müsste:

> *(Rz 54) „Daher muss die fragliche Unionsregelung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen“*

Zudem machte der EuGH deutlich, dass der mit der Richtlinie verbundene Eingriff auf das absolut Notwendigste zu beschränken ist (Rz 56) und bemängelte das Fehlen jeglicher gerichtlicher Kontrolle (Rz 62).

Die vorgeschlagenen Mindestbefugnisse in Art. 8 CPC, umfassen – zumindest im derzeitigen Wortlaut - weitreichende Grundrechtseingriffe ohne die erforderliche Abwägung nach dem Verhältnismäßigkeitsgrundsatz mit einzubeziehen sowie ohne einen effektiven Rechtsschutz zu gewähren.
Die ISPA fordert, dass die geplanten Ermittlungsbefugnisse, welche in die Grundrechte des Einzelnen eingreifen, jedenfalls einer ex-ante gerichtlichen Bewilligung unterliegen. In der aktuellen Ausformung entsprechen die Ermittlungsbefugnisse nicht den Anforderungen der EU-Grundrechtecharta sowie der Rechtsprechung des Europäischen Gerichtshofes und sind in dieser Form daher abzulehnen.

2. Die Unbestimmtheit der Begrifflichkeiten im Verordnungsentwurf bringt Rechtsunsicherheit mit sich

Es bestehen große Zweifel hinsichtlich des tatsächlichen Umfangs der einzelnen Befugnisse aufgrund der zahlreichen unbestimmten Rechtsbegriffe. Insbesondere erfolgt in der Verordnung keine Definition einer "schwerwiegenden und nicht wieder gutzumachenden Schädigung von Verbrauchern" auf welche die Verordnung unter anderem in Art 8 lit. g CPC Bezug nimmt. Das Risiko, einer ausufernden Interpretation des Anwendungsbereichs der Ermittlungsbefugnisse von Kosumentenschutzbehörden ist dadurch immanent und mit den Grundsätzen der Bestimmtheit und der Vorhersehbarkeit von Gesetzen in keinster Weise vereinbar. Hierbei möchte die ISPA noch einmal auf die bereits im vorherigen Punkt zitierte Entscheidung des EuGH in der Rs Digital Rights verweisen, in der dieser „*klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme*", sowie eine Einschränkung auf die Ermittlung, Feststellung und Verfolgung von schweren Straftaten fordert.

Die ISPA regt daher an, dass eine Umsetzung der Richtlinie jedenfalls erst nach einer Konkretisierung der Rechtsbegriffe erfolgen kann, da zuvor auch eine genaue Stellungnahme nur äußerst schwierig und verbunden mit vielen Annahmen möglich ist.

3. Die Beauskunftung von Kundendaten durch ISPs muss jedenfalls den strengen österreichischen Formvorschriften folgen

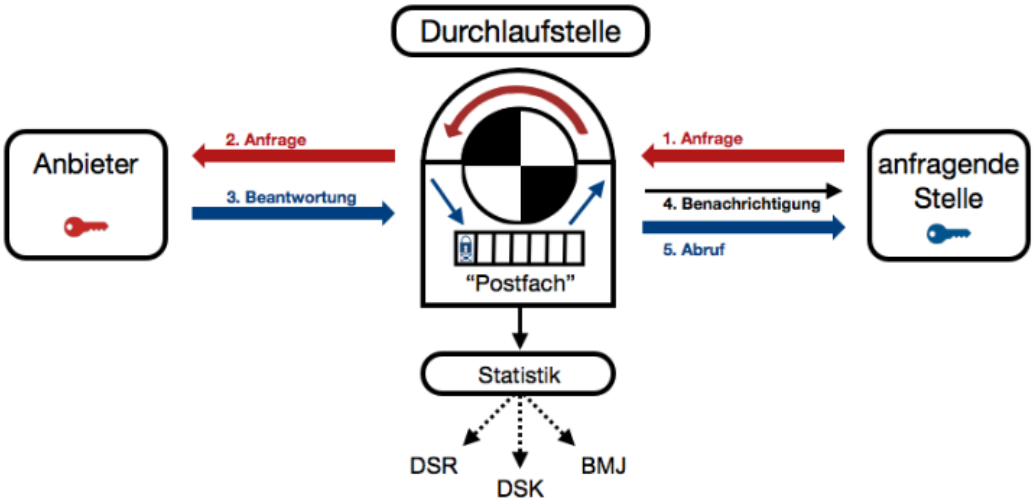
Konsumentenschutzbehörden wird gemäß Art 8 Abs. 2 lit. b CPC die Möglichkeit zur Einholung von jeglicher relevanter Information, Daten oder Dokumenten in jeglichem Format, von Providern eingeräumt. Der Anwendungsbereich für diese Befugnis wird dabei nicht genau umschrieben, sondern es wird nur unter anderem demonstrativ die Rückverfolgung von Daten- und Finanzflüssen, Identitätsfeststellung, sowie die Feststellung der Betreiber von Webseiten als Anwendungsfall aufgezählt. Diese, wiederum sehr vage und offen formulierte Befugnis, umfasst demnach auch die Beauskunftung von Kundendaten durch Provider an Konsumentenschutzbehörden.

Bislang besteht in Österreich eine Beauskunftungsverpflichtung für Provider ausschließlich gegenüber Strafgerichten sowie bestimmten Behörden (u. a. Kriminalpolizei oder Staatsanwaltschaft), sofern es hierzu eine gesetzliche Grundlage im Telekommunikationsgesetz gibt. Eine Ausweitung der Berechtigung zur Einholung von Beauskunftungen auf Teile des Zivilrechts sowie auf weitere Behörden, widerspricht klar der bisher geltenden Abgrenzung.

Die Bereitstellung aller technischen Einrichtungen für eine Beauskunftung stellt für Provider zudem einen großen finanziellen Aufwand dar, wobei die Überwachung des Fernmeldeverkehrs nach den verfassungsrechtlichen Wertungen grundsätzlich Sache des Staates ist. Es wäre daher unverhältnismäßig, wenn der Provider diese Kosten selbst zu tragen hätte weswegen eine entsprechende Bestimmung in jedem Fall einen Kostenersatz, für Provider vorsehen muss. Dies

wurde bereits vom Verfassungsgerichtshof[1] in einem Erkenntnis bestätigt. Zudem sollten Anfragen an gewisse Kostenhürden gebunden werden, damit gewährleistet wird, dass unverhältnismäßige Anfragen unterbunden werden.

Zudem besteht für Provider gemäß § 94 Abs. 4 TKG die Verpflichtung, sensible Daten (Verkehrsdaten, Standortdaten, Stammdaten) nur unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu übermitteln. Hierzu wurde ein elektronisches Postfachsystem zur sicheren Abwicklung von Anfragen und Auskünften (die sogenannte „Durchlaufstelle“, kurz „DLS“) bei der Bundesrechenzentrum GmbH eingerichtet, an welche alle Beteiligten über einen verschlüsselten Übertragungskanal angebunden sind:



Die ISPA lehnt jegliche Unterwanderung dieses etablierten Systems, durch welches die Integrität der übertragenen Daten gewahrt wird und das als „best-practice“ in andere Staaten der EU getragen wird, ab. Es wird angeregt, die bereits in Art 8. Abs.1 CPC enthaltene Formulierung „Each competent authority […] shall exercise them in accordance with this Regulation and national law” näher zu definieren. Dabei muss insbesondere klargestellt werden ob sich dies nur auf das nationale Prozessrecht oder aber auch auf materielles Recht bezieht und ferner, sollte dieses davon nicht umfasst sein, jedenfalls ein Verweis auf die Einhaltung der nationalen Bestimmungen zur sicheren Übertragung von sensiblen Daten durch Provider, aufgenommen werden.

4. Zugangssperren durch Access Provider sind drakonische, kostenintensive Maßnahmen und sind daher abzulehnen

Unter den vorgeschlagenen Mindestbefugnissen für Konsumentenschutzbehörden, findet sich in lit. g, die Befugnis, vorübergehende Maßnahmen zu erlassen, wenn die Gefahr von

[1] Verfassungsgerichtshof, 27.02.2003, G 37/02 ua, V 42/02

schwerwiegenden und nicht wieder gutzumachenden Schädigungen von Verbrauchern besteht. Demonstrativ wird dabei das Sperren von Websites erwähnt. In lit. l wird wiederum die Befugnis zur Anordnung der Löschung von Webseiten oder anderen Online-Diensten vorgesehen.

In der Praxis werden Anordnungen zur Verhängung von Netzsperren durch DNS-Blocking umgesetzt. Dabei muss ein Provider, der für die Durchführung der Benutzerabfragen zuständig ist um den Zugang zu einer bestimmten Website zu blockieren, in die von ihm kontrollierten DNS-Verzeichnisse eingreifen. Damit kann er den Nutzer davon abhalten, die von ihm angeforderte Webseite aufzurufen. Durch eine solche Maßnahme wird der Zugang zu allen Webseiten unter dieser Domain sowie allen Subdomains verunmöglicht.

Da es sich dabei um einen gravierenden Eingriff in die freie Verfügbarkeit von Inhalten im Internet handelt, ist die Anordnung von Netzsperren gemäß Maßgabe des EuGH nur unter sehr strengen Voraussetzungen möglich. Die Internetwirtschaft wehrt seit Jahren diesbezügliche Begehrlichkeiten (welche vornehmlich von Rechteinhaber gefordert werden z.B. IP-Adressen Blocking), auch im Interesse ihren Kundinnen und Kunden ab. Gleichzeitig sieht der Vorschlag der EU-Kommission jedoch nunmehr vor, dass Provider all diese Dinge für Konsumentenschutzbehörden umsetzen müssen. Es besteht daher die Gefahr, dass das langjährige Engagement der Internetwirtschaft gegen die Etablierung von Netzsperren in Österreich hinfällig wird, da nun aufgrund der direkten Anwendung von Bestimmungen einer EU-Verordnung, Netzsperren gewissermaßen durch die „Hintertür“ eingeführt werden könnten. Sollte entgegen der Ansicht der ISPA am Gedanken von Netzsperren festgehalten werden, sind diese daher in der Verordnung ausdrücklich auf DNS Blocking-Maßnahmen zu beschränken.

Weiters besteht ein großes Risiko, dass es zu einer „slippery-slope“ (also einer nicht aufzuhaltenden Ausweitung) kommt. Beispiele in anderen Mitgliedsstaaten haben gezeigt, dass sobald die Sperrinfrastruktur geschaffen wurde, weitere Interessengruppen danach streben werden, diese für sich zu nutzen, jeweils unter dem Vorwand dabei ebenfalls nur bestimmte Rechte schützen zu wollen. Die Auswirkungen auf eine freie Nutzung des Internets wären jedoch fatal. Wie aus einer aktuellen Studie des Europarats hervorgeht, ist Österreich derzeit beispielhaft, für ein Land mit einer überdurchschnittlich gut ausgeprägten Meinungsfreiheit im Internet[2]. Durch die Schaffung von Sperrinfrastruktur würde diese erfreuliche Stellung Österreichs gefährdet werden.

Zudem stellt die Sperrung einer Website einen finanziellen und organisatorischen Aufwand dar, welcher insbesondere von kleinen und mittleren Providern in dieser Form nicht nur nicht tragbar, sondern existenzbedrohend ist.

Die ISPA regt daher dazu an, beide Bestimmungen nur als Anordnung gegenüber dem Hosting-Provider vorzusehen. In diesem Fall, würde eine Anordnung gemäß Art 8 lit g CPC, den Hosting-Provider zu einer vorübergehenden Trennung der Festplatte, auf welcher der Inhalt der illegalen Website gehostet wird, von seinem internen Netzwerk verpflichten. Die Effizienz einer solchen

[2] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680658544

Maßnahme, hinsichtlich des Konsumentenschutzes, ist dabei die gleiche wie bei einem Ansetzen der Sperre auf Seiten des Access-Providers, jedoch mit weit weniger weitreichenden Konsequenzen für ein freies Internet.
Ein Antrag gemäß Art 8 lit. l CPC soll nach Interpretation der ISPA sich ebenfalls gegen den Hosting-Provider richten, wobei in diesem Fall nicht nur die vorrübergehende Trennung der Festplatte sondern die Löschung der darauf befindlichen Daten angeordnet wird. In diesem Fall, wird es dem Betreiber der illegalen Website weit mehr erschwert, die gleiche Website auf einer anderen Domain zu eröffnen, da er nicht mehr über die notwendigen Daten verfügt. Somit würd eine solche Interpretation eine „win-win" Situation, für Access-Provider, Konsumentenschützer und insbesondere Verbraucher bringen.

Hosting-Provider sind in der Regel auf einfache Weise, mit Hilfe von „IP traceback" Instrumenten ausfindig zu machen und befinden sich zumeist, aufgrund der hohen infrastrukturellen Anforderungen, im Gebiet der Europäischen Union. Angesichts der angestrebten Kooperation zwischen den Konsumentenschutzbehörden, sollte eine Anordnung gegenüber einem im EU-Ausland situierten Hosting-Provider daher einfach durchführbar sein.

Um Zweifel der diesbezüglichen Auslegung der Bestimmung zu beseitigen, schlägt die ISPA folgende Formulierung der beiden Bestimmungen vor:

> *Art 8 Abs. 2 lit g:*
> *request interim measures to prevent the risk of serious and irreparable harm to consumers, in particular the temporary take-down of a website, or a similar digital site, service or account by the hosting provider; the interim measures shall not go beyond what is necessary to achieve the objective and shall solely be implemented if no other measures are available to stop the infringement*

> *Art 8 Abs. 2 lit l:*
> *request the permanent take-down of a website or similar digital site, service or account or a part of it, including by requesting a third party or other public authority to implement such measures; such a request shall only be granted for serious infringements and if the measure does not go beyond what is necessary to achieve the objective and shall solely be implemented after an exhaustive attempt to cooperate with the website owner has failed*

5. Netzsperren sind kein effizientes Mittel um Konsumenten vor „fake-shops" und anderen Gefahren zu schützen

Die ISPA ist sich der Gefahren, die sich Konsumenten durch die zum Teil äußerst detailreich konzipierten Betrugs-Websites bietet, bewusst. Jedoch stellt die Anordnung von Netzsperren hierzu nicht das effizienteste Mittel dar, da insbesondere DNS-Sperren vom Betreiber der Website relativ einfach und schnell - etwa durch Änderung der Top-Level Domain - umgangen werden können.

Die ISPA regt vielmehr dazu an, alternative Lösungswege zu beschreiten und möchte dabei auf das sogenannte „follow-the-money“ Prinzip aufmerksam machen: Dabei werden die im Rahmen des Webshops getätigten Zahlungen zurückverfolgt und die entsprechenden Konten gesperrt bzw. das Geld zurücküberwiesen. Auf diese Weise wird den Betreibern von „fake-shops“ mehr Schwierigkeiten bei Zahlungsvorgängen bereitet und diese damit an der Wurzel der Motivation zum Betrieb eines solchen Webshops angegriffen, mit der Folge, dass sich nach einiger Zeit der Aufwand und die immanente Gefahr nicht mehr lohnt. Denn anders als bei für den Nutzer offensichtlich als illegal zu identifizierenden Plattformen im Darknet, auf welchen illegales Material angeboten wird, werden gewöhnliche Kunden keinen Webshop in Anspruch nehmen in welchem über Bitcoins oder ähnliche dezentrale Zahlungssysteme gezahlt wird.

6. Der Terminus „Domain“ soll aus den in Art. 8 genannten Befugnissen ersatzlos gestrichen werden

Die bereits unter Punkt 4. diskutierten Mindestbefugnisse für Konsumentenschutzbehörden sehen auch die Suspendierung bzw. Löschung ganzer Domains vor. Diesbezüglich möchte die ISPA, nach Rücksprache mit der österreichischen Domainvergabestelle nic.at, auf eine Reihe von erheblichen Problemen hinweisen.

Die Löschung oder Suspendierung einer Domain hat enorme Auswirkungen technischer Natur. Bei Sperrung oder Löschung einer Domain, sind davon sämtliche, dahinterliegende Dienste, z.B. auch E-Mail oder Website, betroffen. Dieser Eingriff wirkt sich somit einerseits auf Dienste aus, die über den Inhalt einer Webseite hinausgehen (z.B. E-Mail, FTP-Server, etc.) und andererseits auch auf sämtliche Inhalte der Webseite selbst, die keinerlei Rechtsverletzung beinhalten. Ein gezielter Eingriff von Seiten der Domainvergabestelle hinsichtlich rechtsverletzender Inhalte ist nicht möglich und daher die angedachte Befugnis im Rahmen von Verletzungen von Konsumentenschutzrechten völlig überschießend.

Darüber hinaus möchte die ISPA darauf hinweisen, dass der Vertragsgegenstand zwischen der Domainvergabestelle und dem Domaininhaber bzw. der Domaininhaberin - der auch nicht ident sein muss mit dem Medieninhaber oder dem Betreiber der Webseite - ausschließlich die Domain (also der Domainname in Kombination mit der Top Level Domain – in Österreich .at) ist und keinerlei dahinterliegenden Dienste. Ein gezielter Eingriff in die Inhalte ist der Domainvergabestelle also nicht möglich.

Die ISPA empfiehlt daher, das Wort Domain aus den in Artikel 8 geregelten Mindestbefugnissen ersatzlos zu streichen.

7. **Aufgrund des weitreichenden Anwendungsbereichs der Richtlinie käme es in Österreich zu einer immensen Ausweitung sensibler Eingriffsbefugnisse**

Der Umfang der von der Richtlinie erfassten Behörden wird in der Richtlinie sehr weit gehalten. Gemäß Art 1 iVm Art 3 (a) CPC handelt es sich dabei um jene nationalen Behörden, welche mit der Durchsetzung der im Annex der Richtlinie aufgelisteten europäischen Verbraucherschutzstandards betraut sind. Aufgrund der Vielzahl an unterschiedlichen Rechtsgebieten, welche dabei umfasst sind, würden die im Entwurf vorgesehenen Mindestbefugnisse in Österreich für eine Vielzahl an Behörden vorgesehen werden:

- Das Bundesministerium für Arbeit, Soziales und Konsumentenschutz (als zentrale Verbindungsstelle)
- Bundeswettbewerbsbehörde
- Bundeskartellanwalt
- KommAustria
- Bundesamt für Sicherheit im Gesundheitswesen
- Bundesministerium für Verkehr, Innovation und Technologie
- Die Fernmeldebüros Wien, Linz, Innsbruck & Graz

Insbesondere in Anbetracht der zum Teil äußerst kritischen Eingriffsbefugnisse, möchte die ISPA jedenfalls davor warnen, dass es zu einer unkontrollierten Ausuferung kommt. Bisher sind nach österreichischem Recht, sowohl Beauskunftungsberechtigungen, als auch ähnliche Maßnahmen, ausschließlich für Gerichte bzw. Strafverfolgungsbehörden vorgesehen. Die Ausweitung der Befugnisse auf eine derart große Anzahl weiterer Behörden, wäre ein äußerst gravierender Schritt, welcher im Lichte der enormen Eingriffsintensität gebührend restriktiv gehandhabt werden sollte.

Die ISPA regt daher dazu an, eine differenziertere Definition der durch die Richtlinie berechtigten Behörden vorzusehen, wobei Befugnisse zum Eingriff in sensible Rechte jeweils explizit nur einzelnen Behörden, nach nachweißlicher Ausschöpfunger aller zumutbaren alternativen Mittel, sowie gegen Kostenersatz zugestanden werden soll.

8. **Die datenschutzrechtlichen Bestimmungen bei der Weiterverwendung der gesammelten Daten müssen beibehalten werden**

In Art. 41 ff des Entwurfs wird die Weiterverwendung der, auf Basis der in Art 8 geregelten Ermittlungsmaßnahmen, gesammelten Daten und Informationen geregelt. Die darin enthaltenen Bestimmungen entsprechen weitestgehend den bisherigen Regelungen in Art 13ff der bestehenden Verordnung, jedoch sind einige wesentliche Änderungen festzuhalten die kritisch zu sehen sind. Insbesondere fehlt in Art 41 CPC nunmehr jeglicher Hinweis, auf die Bestimmungen der Datenschutzrichtlinie bzw. deren Nachfolgebestimmungen in der Datenschutzgrundverordnung. In ihrer bisher hierzu ergangenen Kommunikation, hielt die EU-Kommission fest, dass es aufgrund des überarbeiteten EU-Datenschutzrechtes keinen expliziten Hinweis mehr zur Einhaltung der datenschutzrechtlichen Bestimmungen in Art 41 benötigt.

Die ISPA äußert hierzu Bedenken und fordert, speziell aus Gründen der Rechtssicherheit und um Rechtslücken zu verhindern, den Verweis wie im bestehenden Art 13 Abs. 4 CPC zu belassen.

Ferner ist es unverständlich, weshalb die bisher in Art 14 enthaltene Bestimmung, wonach die im Rahmen der Verordnung übermittelten Informationen nur dann an Behörden in Drittstaaten weitergegeben werden können, sofern die Einwilligung der zuständigen Behörde, von der die Informationen ursprünglich stammen, eingeholt wurde, entfernt wurde. Denn es kann nicht davon ausgegangen werden, dass die zuständige Behörde bereits durch die Erteilung der Information der weiteren Verwendung zustimme.

Weiters ist es bedenklich, dass in den Bestimmungen zur Datenbank der EU-Kommission in Art 43 des Entwurfs, die in der bisherigen VO in Art 10 Abs. 2 enthaltene Regelung betreffend die Löschung von Daten - sofern eine zuständige Behörde festgestellt hat, dass sich ein von ihr mitgeteilter innergemeinschaftlicher Verstoß letztlich als unbegründet erwiesen hat – weggefallen ist. Zudem fehlt auch – wie bereits in Art 41, der grundsätzliche Verweis auf das anzuwendende Datenschutzregime, auch in diesem Fall fordert die ISPA aus datenschutzrechtlicher Sicht eine Klarstellung und Beibehaltung eines Verweises.

Zuletzt, möchte die ISPA festhalten, dass die Bestimmungen zur Datenverwendung abschließend in der Verordnung selbst – und nicht wie in Art 43 Abs. 4 vorgesehen in Durchführungsakten der EU-Kommission – zu regeln ist, insbesondere um Rechtssicherheit zu schaffen.

Für Rückfragen oder weitere Auskünfte stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

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 über 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.