An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

Bundeskanzleramt
Ballhausplatz 1
1010 Wien

E-Mail: team.z@bmj.gv.at; medienrecht@bka.gv.at

Wien, am 13. November 2023

STELLUNGNAHME DER ISPA ZUM ENTWURF EINES BUNDESGESETZES, MIT DEM DAS KOORDINATOR-FÜR-DIGITALEDIENSTE-GESETZ ERLASSEN UND DAS KOMMAUSTRIA-GESETZ, DAS E-COMMERCEGESETZ, DAS ALLGEMEINE BÜRGERLICHE GESETZBUCH, DAS URHEBERRECHTSGESETZ, DAS GERICHTSGEBÜHRENGESETZ, DAS MEDIENGESETZ, DIE STRAFPROZEßORDNUNG 1975, DAS STAATSANWALTSCHAFTSGESETZ, DAS EU-JZG, DAS AUSLIEFERUNGS- UND RECHTSHILFEGESETZ UND DAS TELEKOMMUNIKATIONSGESETZ 2021 GEÄNDERT WERDEN (DSA-BEGLEITGESETZ – DSA-BEGG)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, im Rahmen der öffentlichen Konsultation des Entwurfs eines Bundesgesetzes, mit dem das Koordinator-für-digitale Dienste-Gesetz erlassen und das KommAustria-Gesetz, das E-CommerceGesetz, das Allgemeine bürgerliche Gesetzbuch, das Urheberrechtsgesetz, das Gerichtsgebührengesetz, das Mediengesetz, die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz, das EU-JZG, das Auslieferungs- und Rechtshilfegesetz und das Telekommunikationsgesetz 2021 geändert werden (DSA-Begleitgesetz – DSA-BegG) wie folgt Stellung zu nehmen:

Eingangs möchte die ISPA ihr Bedauern über die äußerst kurz bemessene Begutachtungsfrist von nicht einmal drei Wochen zum Ausdruck bringen. Eine derart kurze Frist ist einer fundierten Auseinandersetzung mit dem Entwurf abträglich, vor allem angesichts der Tatsache, dass im Rahmen des Gesetzespakets Änderungen aus verschiedenen Rechtsbereichen gemeinsam konsultiert werden. Dazu kommt, dass aufgrund der in der Begutachtungsfrist gelegenen Feiertage überhaupt nur 11 Werktage für die interne Analyse des Entwurfs sowie die Diskussion der vorgeschlagenen Bestimmungen mit unseren Mitgliedsunternehmen zur Verfügung gestanden sind.

Ein Teil dieser Werktage befand sich zudem in den Herbstferien, in denen gerade die zahlreichen Mitarbeiter:innen mit Kindern im Schulalter sich nicht entsprechend einbringen konnten.

Eine derart kurze Konsultationsfrist ist gerade im Fall der Sektion V des Bundeskanzleramts überraschend, da der darin angesiedelte Verfassungsdienst selbst mehrmals auf die Einhaltung angemessener Begutachtungsfristen gedrängt hat.[1] Auch ist aus einigen Formulierungen der Erläuternden Bemerkungen, etwa der Tatsache, dass darauf hingewiesen wird, dass die Bestimmungen über sehr große Online-Plattformen und Online-Suchmaschinen schon „zuvor" [vor 17. Februar 2024] in Kraft treten, abzuleiten, dass der Entwurf des KDD-G offenbar bereits weitaus früher fertiggestellt worden ist. Denn der DSA ist bereits seit 25. August 2023 auf die entsprechenden Online-Plattformen anwendbar.

Es ist bedauerlich, dass aufgrund der offenbar eingetretenen Verzögerungen bei der Ausarbeitung und internen Abstimmung des Entwurfs nun die Möglichkeit der betroffenen Nutzer:innen und Unternehmen, am Gesetzgebungsprozess durch Übermittlung von fachlichem Input teilzunehmen, erheblich eingeschränkt wird.

Zu § 2 Abs. 1 u. 2 KDD-G bzw. § 47 Abs. 2 TKG 2021

Einige der aus dem Digital Services Act resultierende Pflichten weisen große Überschneidungen mit bereits bestehenden Pflichten für Internetzugangsanbieter auf. So stellt Art. 14 DSA etwa konkrete Anforderungen an die Allgemeinen Geschäftsbedingungen von Anbietern von Vermittlungsdiensten, die darin „Angaben zu etwaigen Beschränkungen in Bezug auf die von den Nutzern bereitgestellten Informationen" aufnehmen müssen. Auch heute schon sind Anbieter von Internetzugangsdiensten gemäß § 132 Abs. 2 Z 12 TKG 2021 iVm Art 4 VO 2015/2120 verpflichtet in ihren AGB transparente Informationen zu den von ihnen ergriffenen Verkehrsmanagementmaßnahmen aufzunehmen, worunter auch Maßnahmen zu verstehen sind, durch welche der Zugriff auf von einem Nutzer bereitgestellte Informationen eingeschränkt wird (Zugangssperren). Zur Prüfung der AGB der Zugangsanbieter ist die Rundfunk und Telekom Regulierungs-GmbH Fachbereich Telekom berufen, die gemäß § 133 Abs. 1 TKG 2021 sämtliche AGB vor Aufnahme des Dienstes bzw. bei jeder Änderung vorgelegt werden müssen.

Darüber hinaus obliegt der Telekom-Control-Kommission gemäß §§ 47 u. 198 Z 23 TKG 2021 iVm Art. 5 Abs. 1 Verordnung (EU) 2015/2120 die Aufsicht über geeignete und erforderliche Verkehrsmanagementmaßnahmen im Einzelfall, wozu insbesondere auch die Einrichtung von Zugangssperren zählt. In diesem Zusammenhang erscheint es jedoch unklar, inwiefern durch die angedachte Novellierung in § 47 Abs. 2 TKG 2021 in Hinkunft auch die KommAustria in diese Verfahren miteinbezogen wird. Denn darin ist vorgesehen, dass das Einvernehmen mit der KommAustria immer dann notwendig sein soll, wenn durch die zu beurteilende Verkehrsmanagementmaßnahme Zuständigkeiten „wie insbesondere jene nach § 199 Abs. 4a" betroffen sind, wozu in Hinkunft die Wahrnehmung sämtlicher Befugnisse und Aufgaben nach dem

[1] Vgl etwa Rundschreiben des Verfassungsdiensts betreffend Festsetzung angemessener Begutachtungsfristen (GZ BKA-600.614/0002-V/2/2008)

DSA zählen. Da wie oben ausgeführt Verkehrsmanagementmaßnahmen durch Anbieter von Internetzugangsdiensten stets auch Inhaltsmoderationsmaßnahmen im Sinne des Art 14 DSA darstellen, hätte dies zur Folge, dass zur Beurteilung dieser Maßnahmen in Hinkunft stets zwei Behörden eingebunden werden. Dies kann nicht im Sinne des verwaltungsrechtlichen Effizienzgebots sein.

Um daher für eine einheitliche Rechtsauslegung zu sorgen sowie den Aufwand auf Seiten der Behörden in einem angemessenen Rahmen zu halten regt die ISPA eine Ergänzung in § 2 KDD-G an, wonach in jenen Belangen, welche ausschließlich Anbieter von Internetzugangsdiensten betreffen, weiterhin eine Zuständigkeit der Telekom-Regulierungsbehörden, der RTR-GmbH Fachbereich Telekom sowie der Telekom-Control-Kommission, bestehen bliebt.

Darüber hinaus regt die ISPA im Sinne der besseren Verständlichkeit auch an, in § 47 Abs. 2 TKG 2021 keinen generellen Verweis auf „Zuständigkeiten nach § 199 Abs. 4a“ aufzunehmen, sondern lediglich die Wortfolge „Kommunikationsplattformen im Sinne des § 2 Z 4 des Kommunikationsplattformen-Gesetzes (KoPl-G)“ durch die Wortfolge „Online-Plattform im Sinne des Art. 3 lit. i der Verordnung (EU) Nr. 2022/2065“ zu ersetzen.

Zu § 2 Abs. 3 KDD-G

Eine der Aufgaben der KommAustria soll in Hinkunft die Zuerkennung sowie der Widerruf des Status als vertrauenswürdiger Hinweisgeber gemäß Art. 22 Abs. 2 DSA sein. Vertrauenswürdige Hinweisgeber bzw. „trusted flagger“, deren Meldungen priorisiert behandelt werden, stellen heute schon einen entscheidenden Faktor beim Kampf gegen Hass im Netz bzw. illegale Inhalte dar. Wie aus der Bezeichnung wörtlich hervorgeht, ist das Charakteristikum eines trusted flaggers das Vertrauen, welches Online-Plattformen diesen Organisationen entgegenbringen. Diese Vertrauenswürdigkeit lässt sich in vielen Fällen an der Qualität der bisherigen Meldungen der entsprechenden Institutionen messen, worüber die betroffenen Diensteanbieter am besten Auskunft geben können. Ebenso bezieht sich die Sachkenntnis der Antragsteller sehr häufig auf einzelne Mitgliedstaaten und nicht das gesamte Unionsgebiet.

Die ISPA regt daher an, im Rahmen des Zuerkennungsverfahrens gemäß Art 22 Abs. 2 DSA auch den betroffenen Diensteanbietern die Möglichkeit zu geben, ihre bisherigen Erfahrungen mit den Meldungen der antragstellenden Institutionen darzulegen um die Behörde bei der Beurteilung der Bedingungen gemäß Art 22 Abs. 2 lit. a) bis c) zu unterstützen. Darüber hinaus sollten Antragsteller ihre Sachkenntnis in Bezug auf einzelne Mitgliedstaaten jeweils durch Darlegung ihrer Erfahrung in der Beurteilung und Meldung von illegalen Inhalten über einen Zeitraum von mindestens sechs Monaten untermauern. Damit würde auch die Anzahl der EU-weiten vertrauenswürdigen Hinweisgeber, die durch die KommAustria verwaltet werden, begrenzt und die Effektivität gesteigert werden.

Zu § 4 KDD-G

In Umsetzung von Art 51 Abs. 3 lit. b DSA ist angedacht, dass die KommAustria in Hinkunft vor dem Bundesverwaltungsgericht einen Antrag auf vorrübergehende Sperre des Zugangs zu einem Vermittlungsdienst bzw. einer Online-Schnittstelle stellen kann, sofern alle anderen Befugnisse zur Einstellung einer Zuwiderhandlung ausgeschöpft sind, die Zuwiderhandlung nicht behoben wurde oder anhält und einen schwerwiegenden Schaden verursacht, der durch die Ausübung anderer Befugnisse nicht vermieden werden kann. Angesichts der sehr eng gesteckten Voraussetzungen geht die ISPA davon aus, dass entsprechende Anordnungen nur in Ausnahmefällen erlassen werden. Dennoch erscheint die konkrete Umsetzung der Bestimmung unklar.

Zum einen geht aus der Bestimmung nicht hervor wie die Internetzugangsanbieter, die letztlich die Anordnung umsetzen müssen, über die Entscheidung des BVwG informiert werden bzw. inwiefern die Entscheidung des Gerichts ihnen gegenüber Rechtswirkung entfaltet. Die ISPA möchte an dieser Stelle daran erinnern, dass Anbieter von Internetzugangsdiensten den Zugang zu einem Vermittlungsdienst oder einer Online-Schnittstelle nur unter ganz bestimmten Voraussetzungen sperren dürfen die abschließend in Art 3 Abs. 3 TSM-VO[2] geregelt sind. Daraus geht hervor, dass entsprechende Verkehrsmanagementmaßnahmen – abgesehen von technischen Gründen – nur ergriffen werden dürfen, wenn sich eine entsprechende Pflicht direkt aus einem Rechtsakt oder einer darauf basierenden Entscheidung eines Gerichts oder einer Verwaltungsbehörde ergibt. Da die entsprechende Pflicht in diesem Fall nicht eindeutig aus Art 51 DSA bzw. § 4 KDD-G hervorgeht ist es daher erforderlich, dass der Zugangsdiensteanbieter selbst Adressat einer entsprechenden Anordnung ist, um sich auf diese als Rechtsgrundlage für die Verkehrsmanagementmaßnahme berufen zu können.

Gesetzlich zur Überprüfung von Verkehrsmanagementmaßnahmen berufen ist gemäß Art 5 TSM-VO die Telekom-Control-Kommission, die hierzu in einer Reihe von Entscheidungen entsprechendes Fachwissen aufgebaut hat. Dazu gehört insbesondere auch die Prüfung der technischen Umsetzung der Maßnahme. Aus diesem Grund wurde die TKK auch bereits an anderer Stelle, etwa für die Beurteilung eines Antrags auf Sperre einer Online-Schnittstelle aus Gründen des Verbraucherschutzes als zuständige Behörde vorgesehen.[3]

Darüber hinaus erscheint es generell fraglich, ob das vorgesehene Verfahren im Einklang mit den Vorgaben eines effektiven Rechtschutzes in Art. 6 der Europäischen Menschenrechtskonvention (EMRK) bzw. Art. 47 der Charta der Grundrechte der Europäischen Union (GRC) wäre. Denn den Betroffenen steht im Fall der Entscheidung des BVwGs als Rechtsmittel lediglich die Revision an den Verwaltungsgerichtshof zur Verfügung, die jedoch nur unter den in Art 133 Abs. 4 B-VG enthaltenen, eingeschränkten Voraussetzungen zulässig ist. Darüber hinaus ist der VwGH an die Sachverhaltsfeststellung des BVwGs gebunden. Diese Einschränkungen im Rahmen der Revision waren aber gerade mit dafür verantwortlich, dass das Bundesverwaltungsgericht im Rahmen der

[2] Verordnung 2015/2120 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union

[3] Vgl Bundesgesetz über die Zusammenarbeit von Behörden im Verbraucherschutz (VerbraucherbehördenKooperationsgesetz – VBKG) § 7b

Verwaltungsgerichtsbarkeits-Novelle 2012 ins Leben gerufen wurde, um den Rechtsschutz im gesamten Verwaltungsverfahrenswesen zu stärken. Indem nun das Verfahren in erster Instanz selbst beim BVwG angesiedelt wird, ergibt sich erneut das Problem, dass als Rechtsmittel lediglich die Revision an den VwGH möglich ist.

Während Art. 6 EMRK sich zwar nur auf zivilrechtliche und strafrechtliche Ansprüche bezieht, gilt die in Art. 47 GRC festgelegte Gewährleistung des effektiven Rechtsschutzes für den Schutz sämtlicher durch das Unionsrecht garantierten Rechte und Freiheiten und damit auch die durch die Sperre eines Vermittlungsdienstes betroffenen Rechte auf freien Informationszugang (Art. 11 GRC), unternehmerische Freiheit (Art. 16 GRC) sowie Eigentum (Art. 17 GRC).

Um daher sowohl den Bedenken aufgrund von Art 47 GRC bzw. Art 6 EMRK zu begegnen als auch um die vorhandene Fachkenntnis zu nutzen, regt die ISPA an, dass die Telekom-Control-Kommission zur Erlassung entsprechender Anordnungen gemäß § 4 KDD-G berufen wird und auf Antrag der KommAustria tätig wird. Das Bundesverwaltungsgericht wäre in diesem Fall gemäß § 200 Abs. 7 TKG 2021 die erste Rechtsmittelinstanz.

Zu §§ 5 u. 6 KDD-G:

Zur Darstellung der Verwaltungsstraftatbestände

Die ISPA sieht die gewählte Form der Darstellung der Verwaltungsstraftatbestände und -sanktionen in §§ 5 u. 6 KDD-G kritisch. Der Entwurf enthält in § 5 eine ausführliche Auflistung jener Verstöße gegen Pflichten aus dem DSA, die eine Verwaltungsübertretung darstellen. Die Strafdrohungen wiederum sind in § 6 des Entwurfs vorgesehen. Anstelle jedoch die einzelnen Straftatbestände des § 5 aufzulisten und jeweils einem bestimmten Strafrahmen zuzuordnen, differenziert § 6 Abs. 1 nach vier unterschiedlichen Fällen (Bereitstellung unrichtiger, unvollständiger oder irreführender Informationen; Unterlassung einer Antwort oder der Berichtigung unrichtiger, unvollständiger oder irreführender Informationen; Nichtduldung einer Nachprüfung; alle anderen Fälle) und ordnet diesen eine bestimmte Strafsanktion zu. Die Rechtsunterworfenen müssen daher durch Auslegung selbst ermitteln, in welche dieser vier Kategorien ein bestimmter in § 5 KDD aufgelisteter Straftatbestand fällt, um den Strafrahmen für den Verstoß zu erfahren. Dies ist legistisch bereits für sich betrachtet kein transparenter Zugang, doch führt er in der Praxis zu noch größeren Schwierigkeiten. Denn bei zahlreichen der in § 5 KDD-G aufgelisteten Straftatbeständen ist nämlich schlichtweg nicht klar, unter welche der vier in § 6 KDD-G vorhandenen Kategorien diese einzuordnen sind. Dies soll anhand zweier Beispiele demonstriert werden:

Gemäß § 5 Abs. 1 Z. 2 KDD-G begeht der Anbieter eines Vermittlungsdienstes eine Verwaltungsstraftat, wenn er einen betroffenen Nutzer entgegen Art. 9 Abs. 5 DSA nicht über die erhaltene Anordnung zum Vorgehen gegen bestimmte rechtswidrige Inhalte und deren Ausführung informiert. Es ist fraglich, ob dieser Fall einer unterbliebenen Information ein Fall der „Bereitstellung unrichtiger, unvollständiger oder irreführender Informationen“ gemäß § 6 Abs. 1 Z. 1 lit. a KDD-G wäre, der mit einer Geldstrafe von bis zu 1% des jährlichen weltweiten Jahresumsatzes zu sanktioniert wird, oder – da nicht nur unvollständige, sondern überhaupt keine Informationen

bereitgestellt wurden – einer von „allen anderen Fällen“ gem. § 6 Abs. 1 Z. 2 KDD-G-E, in welchem Fall die Geldstrafe 6% des weltweiten Jahresumsatzes beträgt.

Gemäß § 5 Abs. 2 Z. 6 KDD-G wiederum begehen Hostingdiensteanbieter (einschließlich Anbieter von Online-Plattformen) eine Verwaltungsübertretung, wenn sie entgegen Art. 17 Abs. 1 lit. a bis d DSA betroffen Nutzern keine klare und spezifische Begründung für relevante Beschränkungen vorlegen. Es ist aber unklar, ob beispielsweise eine unvollständige, unklare oder unspezifische Begründung als unrichtige, unvollständige oder irreführende Information iSd § 6 Abs. 1 Z. 1 lit. a KDD-G zu verstehen ist (in welchem Fall der Strafrahmen von bis zu 1% des Jahresumsatzes anwendbar wäre) oder ob diese Verwaltungsübertretung unter § 6 Abs. 1 Z. 2 KDD-G fällt (in welchem Fall der Strafrahmen von bis zu 6% des Jahresumsatzes anwendbar wäre).

Derartige unklare Fälle finden sich zahlreich in der Auflistung des § 5 KDD-G. Aus dem strafrechtlichen Bestimmtheitsgrundsatz (Vorhersehbarkeitsgebot) gemäß Art 7 EMRK geht jedoch hervor, dass eine Strafnorm den Rechtsunterworfenen eine klare Vorstellung darüber geben muss, welche Folgen mit einem bestimmten Handeln oder Unterlassen verbunden sind. Dies scheint in den erwähnten Fällen jedoch fraglich zu sein, weil gerade nicht klar ersichtlich ist, welche der sich eklatant unterscheidenden Strafdrohungen für das fragliche Verhalten einschlägig sind. Auch ungeachtet der grundrechtlichen Dimension sind mit der gewählten Darstellung der Verwaltungsstrafnormen Auslegungsstreitigkeiten vorprogrammiert, die aus Sicht der ISPA leicht vermeidbar wären. Zwar folgen die in § 6 Abs. 1 angeführten direkt aus Art. 52 Abs. 3 DSA, es spricht aber nichts dagegen, dass der österreichische Gesetzgeber die jeweiligen Verwaltungsübertretungen diesen Fällen zuordnet und die Strafzumessung konkretisiert. So könnten die in § 5 KDD-G enthaltenen Verwaltungsstraftatbestände in Gruppen nach der Höhe der Strafdrohung gegliedert werden (siehe als Beispiele etwa § 188 TKG 2021 oder § 99 StVO). Dies wäre nicht nur anwendungsfreundlicher, sondern würde auch Auslegungsschwierigkeiten hintanhalten. Der Referentenentwurf des deutschen Bundesministeriums für Digitales und Verkehr zum deutschen Umsetzungsgesetz des DSA beinhaltet etwa eine derartige unmittelbare Zuordnung der Strafsanktionen zu den jeweiligen Strafnormen.[4] Die ISPA plädiert dafür, diesen sinnvollen Zugang auch im österreichischen Begleitgesetz vorzusehen.

Zur Ausdifferenzierung der Strafrahmen

Ein weiterer Kritikpunkt der ISPA betrifft die Tatsache, dass der österreichische Gesetzgeber die sehr weiten Strafrahmen von Art. 52 DSA übernommen hat, ohne diese weiter auszudifferenzieren. Der österreichische Entwurf sieht für die in § 5 KDD-G aufgezählten Verwaltungsübertretungen in § 6 Abs. 1 KDD-G-E eine Höchststrafe von bis zu 1% bzw. 6% des jährlichen Einkommens oder

[4] Vgl. Referentenentwurf des Bundesministeriums für Digitales und Verkehr, Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze, § 25 Abs. 4ff Digitale-Dienste-Gesetz, online abrufbar unter https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-20/gesetz-durchfuehrung-verordnung-binnenmarkt-digitale-dienste.html (Stand 31.10.2023).

weltweiten Jahresumsatzes des betroffenen Anbieters von Vermittlungsdiensten oder der betreffenden anderen Person im vorangegangenen Geschäftsjahr vor.

Gerade im österreichischen Umfeld gibt es unzählige kleinere Anbieter von Vermittlungsdiensten (insbesondere Access- und Hosting-Dienste-Anbieter), die den Verpflichtungen des DSA unterliegen. Auch wenn jeder dieser Anbieter guten Willens ist, die Vorgaben rechtskonform zu implementieren, können vereinzelte Verstöße in der Praxis schon aufgrund der schieren Menge und Komplexität der Pflichten vorkommen. Gerade bei kleineren Anbietern sind Übertretungen wie verspätete Meldungen oder dergleichen in ihren tatsächlichen Auswirkungen relativ überschaubar, weshalb aus Gründen der Verhältnismäßigkeit nur eine geringe Geldstrafe bzw. auch eine bloße Verwarnung indiziert sein kann. Es wäre nach Ansicht der ISPA daher nicht angemessen, in derartigen Fällen die Entscheidung über die tatsächliche Höhe der Geldstrafe allein in die Obhut des Koordinators für digitale Dienste zu übertragen und als einzige Begrenzung die erwähnten Maximalbeträge nach § 6 Abs. 1 KDD-G iVm Art. 52 DSA vorzusehen. Vielmehr sollte bereits im österreichischen Begleitgesetz eine Abstufung der maximalen Geldstrafen nach Unternehmensgröße bzw. Umsatz vorgenommen werden und die erwähnten 1% bzw. 6% nur für sehr große Unternehmen anwendbar sein.

Unionsrechtlich wäre dies zulässig, verpflichtet Art. 52 DSA die Mitgliedstaaten doch lediglich dazu, in ihren nationalen Vorschriften dafür zu sorgen, dass die Höchstbeträge von 1% bzw. 6% nicht überschritten werden. Der DSA untersagt es jedoch nicht, dass die Mitgliedstaaten innerhalb dieser Höchstgrenze die Strafdrohungen weiter ausdifferenzieren, wie dies auch der Referentenentwurf des deutschen Bundesministeriums zum Begleitgesetz zum DSA[5] vorsieht. Die ISPA fordert den österreichischen Gesetzgeber auf, sich hier am deutschen Vorbild zu orientieren und eine auf das österreichische Marktumfeld passende Ausdifferenzierung nach Jahresumsätzen vorzunehmen, indem für klein- und mittelgroße Unternehmen im Sinne der EU-Empfehlung 2003/361[6] Abstufungen vorgenommen werden, und die Höchststrafen erst bei Unternehmen mit einem Jahresumsatz von mehr als EUR 50 Millionen zur Anwendung kommen.

In diesem Zusammenhang sollte der österreichische Gesetzgeber auch die einzelnen Verwaltungsübertretungen nach deren Unrechtsgehalt kategorisieren und dementsprechend abgestufte Strafdrohungen vorsehen. Ein Verstoß gegen das Verbot einer täuschenden bzw. manipulativen Konzeption einer Online-Schnittstelle gem. Art. 25 Abs. 1 DSA iVm § 5 Abs. 4 Z. 13 KDD-G ist etwa anders zu gewichten als eine geringfügig verspätete Veröffentlichung des jährlichen Berichts über die durchgeführte Inhaltsmoderation gem. Art. 15 Abs. 1 lit. a bis e und Abs. 2 DSA iVm § 5 Abs. 1 Z 16 KDD-G-E und sollte daher auch unterschiedlichen Strafrahmen unterliegen. Diese Wertungsentscheidung über die Gewichtung der Verwaltungsübertretungen sollte aus Gründen der Vorhersehbarkeit und einheitlichen Rechtsanwendung nicht in jedem Verwaltungsstrafverfahren im Einzelfall dem Koordinator für digitale Dienste überlassen werden, sondern ex ante vom österreichischen Gesetzgeber getroffen werden.

[5] Vgl. ebd.
[6] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen

Dieser Weg wurde auch im Terrorinhalte-Bekämpfungs-Gesetz (TIB-G)[7], dem österreichischen Begleitgesetz zur Verordnung der EU zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (TCO-V)[8] gewählt. Während das Unionsrecht in Art. 18 Abs. 3 TCO-V ebenfalls lediglich eine Obergrenze iHv 4% des weltweiten Jahresumsatzes für systematische oder fortwährende Verstöße gegen die Pflichten aus der Verordnung normiert wurde, hat der österreichische Gesetzgeber in § 7 TIB-G die Pflichten nach deren Unrechtsgehalt gewichtet und ihnen abgestufte Höchststrafen zugeordnet. Auf diese Weise erhält die für Verwaltungsstrafverfahren nach TIB-G zuständige Behörde eine klare Vorgabe über den Strafrahmen für jeden Verstoß gegen Pflichten aus der TCO-Verordnung.

Die ISPA plädiert daher dafür, auch im KDD-G eine klare Differenzierung der einzelnen Verwaltungsübertretungen des DSA vorzunehmen und die Höchststrafen dementsprechend in angemessener Weise abzustufen. Um kleinere Unternehmen nicht zu benachteiligen, sollten keine absoluten Beträge gewählt werden, sondern eine Orientierung am Jahresumsatz erfolgen. Dadurch erhält der Koordinator für digitale Dienste eine klare Rahmenvorgabe, was der Vorhersehbarkeit für die Rechtsanwender:innen und der Einheitlichkeit der Rechtsanwendung zuträglich ist.

Zu Verwaltungsübertretungen iZm der Meldepflicht nach Art. 18 DSA

Ein weiterer Kritikpunkt der ISPA betrifft die Gefahr, dass der gegenständliche Entwurf Anbieter von Hostingdiensten durch hohe Strafdrohungen zu überschießenden Meldungen animiert. Art.18 DSA verpflichtet Hostingdiensteanbieter, die Kenntnis von Informationen erhalten, die den Verdacht begründen, dass eine Straftat, die Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellt, begangen wurde, begangen wird oder begangen werden könnte, zur unverzüglichen Mitteilung an die zuständigen Strafverfolgungs- und Justizbehörden. Der Verstoß gegen diese Verpflichtung ist in § 5 Abs. 2 Z 8 KDD-G iVm § 6 Abs. 1 Z. 1 lit. a KDD-G mit einer Geldstrafe von bis zu 1% des weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr sanktioniert. Aus Sicht der ISPA ist eine derartig hohe Strafdrohung für diese Verpflichtung kritisch zu sehen. Die einzelnen Voraussetzungen des Art. 18 DSA sind nämlich sehr unklar formuliert. Wie stichhaltig muss etwa der angesprochene Verdacht sein, damit eine Meldepflicht ausgelöst wird? Ist jede mögliche – auch nur abstrakte – Gefahr für Leben und Sicherheit einer Person relevant oder gibt es eine Erheblichkeitsschwelle? Geht es bei einer „Gefahr für die Sicherheit einer Person“ nur um die körperliche Integrität und Gesundheit oder ist von einem umfassenderen Sicherheitsbegriff auszugehen? Nach welchen Kriterien ist etwas als „Straftat“ zu beurteilen: Ist hier– neben den in ErwGr. 56 DSA demonstrativ aufgezählten EU-Richtlinien – auch das nationale Strafrecht aller 27 EU-Mitgliedstaaten zu berücksichtigen? Eine Meldepflicht mit derartig komplexen Voraussetzungen in Verbindung mit derart strengen Sanktionen bietet den betroffenen Anbietern große Anreize, bei jeglichen minimalen Indizien eine entsprechende Meldung zu erstatten, um der Gefahr einer Verwaltungsstrafe zu entgehen. Dies würde aber angesichts der enormen Menge an Inhalten, die täglich auf Hostingdiensten (inklusive Online-Plattformen) hochgeladen werden, von denen ein

[7] Bundesgesetz zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (TerrorinhalteBekämpfungs-Gesetz – TIB-G) StF: BGBl. I Nr. 80/2023

[8] Verordnung (EU) 784/2021 des Europäischen Parlaments und des Rates vom 29.4.2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte, ABl. Nr. L 172 vom 17.05.2021 S. 78, online abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX%3A32021R0784

erheblicher Teil auch etwa mittels Meldeverfahren oder eigene Content-Moderation den Anbietern zur Kenntnis gelangt, zu einer Überlastung der Strafverfolgungs- und Justizbehörden führen, die nicht im Sinne des Gesetzgebers sein kann.

Ebenso ist aber unklar, was unter dem Begriff „einschlägige Informationen" zu verstehen ist, die den Strafverfolgungsbehörden zu übermitteln sind. Gemäß ErwGr 56 DSA sind davon „gegebenenfalls" auch Informationen umfasst „die erforderlich sind, um den betreffenden Nutzer ausfindig zu machen und zu identifizieren." Derartige Informationen stellen jedoch personenbezogene Daten dar. Irrt der Hostingdiensteanbieter daher bei der Einstufung eines Inhalts – wobei wie dargelegt schon die Parameter zur Einstufung der Inhalte völlig unklar sind – riskiert er eine Datenschutzverletzung und damit einer erheblichen Geldstrafe nach den Maßstäben der Datenschutzgrundverordnung.

Auch wenn die Ursache des Problems hier im Unionsrecht zu finden ist und letztlich nur der EuGH zur Klärung der Voraussetzungen des Art. 18 DSA berufen ist, kann das Problem auf nationaler Ebene zumindest abgemildert werden. Zum einen ist der Koordinator für digitale Dienste dazu aufgerufen, hier eine verhältnismäßige Rechtsanwendung vorzunehmen und bei einer etwaigen Strafbemessung Rücksicht auf die Komplexität der Rechtslage nehmen. Auch sollte schnellstmöglich im Rahmen des Europäischen Gremium für digitale Dienste eine einheitliche Auslegung des Art. 18 DSA ermittelt werden, welche den damit verbundenen Schwierigkeiten für die betroffenen Anbieter Rechnung trägt. Auch die Erstellung von entsprechenden Leitlinien iSd Art. 61 Abs. 2 lit. b DSA unter Einbindung der relevanten Stakeholder wäre erforderlich. Zum anderen sollte der österreichische Gesetzgeber im Rahmen der von der ISPA geforderten Ausdifferenzierung des Strafrahmens der jeweiligen Verwaltungsübertretungen eine angemessene, nicht zu hohe Strafdrohung für einen Verstoß gegen die Pflichten des Art. 18 DSA vorsehen. Damit kann der Anreiz für Anbieter, übereilte Meldungen zu legen, erheblich vermindert werden.

Zu § 13 ECG

§ 13 ECG entspricht im Wesentlichen dem bisherigen § 18 ECG, mit der Maßgabe, dass sämtliche Auskunftsansprüche nun auf „Vermittlungsdiensteanbieter" im Sinne des Art 3 lit. g. DSA anwendbar sein sollen.

Dies beinhaltet zum einen die Auskunftspflichten gegenüber Gerichten und Verwaltungsbehörden die bislang in § 18 Abs. 2. u. 3 ECG geregelt waren (nun § 13 Abs. Abs. 1 u. 2 ECG). Für diese Auskunftsanordnungen sieht Art. 10 Abs. 2 DSA besondere inhaltliche Vorgaben vor, etwa Angaben welche die Identifizierung des Nutzers ermöglichen bzw. grundsätzlich auch eine Begründung, wozu die Informationen benötigt werden. Zwar gilt Art. 10 Abs. 2 DSA ohnehin unmittelbar in Österreich, dennoch regt die ISPA an, einen entsprechenden Verweis auf die inhaltlichen Anforderungen auch in § 13 Abs. 1 u. 2 ECG aufzunehmen, um für Klarheit bei der Rechtsanwendung zu sorgen.

Darüber hinaus zählt zu den Auskunftspflichten der derzeit in § 18 Abs. 4 ECG enthaltene Auskunftsanspruch Privater, mit dem Diensteanbieter zur Auskunft über Name und Adresse eines Nutzers verpflichten werden können, sofern der Anspruchsteller glaubhaft machen kann, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

Während dieser Anspruch bislang ex lege auf Anbieter von Hosting-Diensten beschränkt war, hat der Oberste Gerichtshof in seiner Rechtsprechung bereits frühzeitig den Anspruch unter bestimmten Voraussetzungen auch auf Telefonie-[9] bzw. E-Mailanbieter[10] ausgeweitet. Durch die Verwendung des Begriffs „Vermittlungsdiensteanbieter“ würde der Anspruch nun jedoch ex lege auch auf andere Anbieter, insbesondere Anbieter von Internetzugangsdiensten, ausgeweitet werden. In diesem Zusammenhang möchte die ISPA darauf hinweisen, dass der Oberste Gerichtshof sich bereits in Bezug auf § 87b Abs. 3 UrhG mit der Frage der Zulässigkeit eines Auskunftsanspruchs Privater gegenüber Access Providern auseinandergesetzt hat und dabei zu dem Ergebnis gekommen ist, dass ein solcher nicht zusteht, da ein Access Provider, um Auskunft über Name und Adresse eines Nutzers zu geben, dem eine IP-Adresse zugeordnet ist, Verkehrsdaten zu Auskunftszwecken verarbeiten muss. Die Fälle in denen dies zulässig ist sind in § 167 Abs. 5 TKG 2021 – in Umsetzung von Art 15 Abs. 1 E-Privacy-RL – taxativ aufgelistet.[11]

Die ISPA ersucht den Gesetzgeber daher, im Rahmen der EBs klarzustellen, dass der Auskunftsanspruch gem. § 13 Abs. 3 ECG auch in Hinkunft nicht gegenüber Access Providern durchgesetzt werden kann bzw. einen Verweis auf die dazu ergangene Rechtsprechung des OGHs – wie auch an zahlreichen anderen Stellen der EBs – aufzunehmen, um angemessene Klarheit zu schaffen.

Zu § 14 ECG

Richtigerweise verweist der Gesetzgeber in den Erläuternden Bemerkungen zu § 14 ECG darauf, dass auch bereits für Auskunftsansprüche nach dem bisherigen § 18 Abs 4 ECG das Herkunftslandprinzip gilt, und § 13 Abs. 3 ECG damit gegenüber Diensteanbietern mit Sitz in einem anderen Mitgliedstaat unangewendet zu bleiben hat, sofern der Diensteanbieter durch die Anordnung einer strengeren Rechtsvorschrift unterworfen wird, als das Recht des Sitzstaates vorsieht. Da die Geltendmachung des Anspruchs jedoch im außerstreitigen Rechtsweg erfolgt und daher an keine Vertretungspflicht gebunden ist, ist dieser Umstand den Betroffenen oftmals nicht bewusst.

Um daher für mehr Klarheit beim Rechtsanwender zu sorgen regt die ISPA an, den Verweis auf die Geltung des Herkunftslandprinzips iSd § 20 ECG bei Anfragen an Diensteanbietern in anderen Mitgliedstaaten, bereits in den Normtext des § 14 ECG (oder alternativ § 13 Abs. 3 ECG) aufzunehmen.

Zu § 15 ECG

Mit der in § 15 ECG neu aufgenommenen Möglichkeit, Anbieter von Vermittlungsdiensten bereits vor Zustellung einer Entfernungsanordnung die Möglichkeit zu geben auf diese zu reagieren und

[9] RS0118691
[10] 6 Ob 226/19g
[11] 4 Ob 41/09x, 6 Ob 119/11k

den Inhalt zu löschen, möchte der Gesetzgeber die rasche Entfernung von Hass im Netz weiter unterstützen.

Während die ISPA das bereits im Zuge des Hass-im-Netz-Bekämpfungsgesetzes[12] in § 549 ZPO eingeführte Mandatsverfahren begrüßt, ist fraglich, ob durch die nun in § 15 ECG geschaffene Möglichkeit tatsächlich ein Mehrwert geschaffen wird. Denn grundsätzlich wird ein Verfahren zum Erlass einer Entfernungsanordnung in aller Regel erst bzw. nur dann eingeleitet, wenn die zuvor ergangene Meldung des Inhalts beim betroffenen Diensteanbieter nicht zum angestrebten Erfolg geführt hat. Um eine solche Meldung möglichst rasch behandeln zu können sollte jedenfalls das in Art 16 DSA vorgesehene Meldeverfahren genutzt werden. Ein Medienbruch durch die Übermittlung einer Meldung per E-Mail führt lediglich zu einer Verzögerung bei der Bearbeitung der Meldung.

Entfernt jedoch ein Vermittlungsdiensteanbieter einen Inhalt aufgrund einer Meldung nicht, dann nur dann, wenn es ihm gemäß Art 16 Abs. 3 DSA ohne eingehende rechtliche Prüfung nicht möglich ist festzustellen, dass die einschlägige Tätigkeit oder Information rechtswidrig ist. Da der Vermittlungsdiensteanbieter sich in diesem Fall nicht auf die Meldung alleine verlassen kann, um die Rechtswidrigkeit zu beurteilen, benötigt er eine konkrete rechtsverbindliche Entscheidung auf die er sich als Rechtsgrundlage für die Entfernung stützen kann. Damit diese jedoch Rechtswirkung gegenüber dem Diensteanbieter entfaltet muss sie auch korrekt, im Einklang mit den Vorgaben der Europäischen Zustellverordnung, zugestellt werden. Als Reaktion auf die Übermittlung per E-Mail könnte der Diensteanbieter daher im Einklang mit Art 9 DSA zumeist nur rückmelden, dass um Zustellung der Entfernungsanordnung ersucht wird, um der Anordnung nachkommen zu können. Da die Nichtbefolgung von Art 9 DSA darüber hinaus auch strafbewehrt ist, stellt sich schließlich auch die Frage, wie der Nachweis erbracht werden kann, dass die Entfernungsanordnung beim betroffenen Diensteanbieter tatsächlich im Sinne des Art 9 Abs. 1 DSA „eingegangen“ ist, da bei der Übermittlung per E-Mail stets die Gefahr besteht, dass von einem Spam-Filter erfasst wird bevor sie vom Diensteanbieter überhaupt abgerufen werden kann.

Ebenso sprechen aber auch Sicherheitsbedenken gegen eine Übermittlung der Entscheidung per E-Mail an den Diensteanbieter. Zum einen kann eine solche E-Mail mittels E-Mail-Spoofing sehr einfach gefälscht werden. Ein Diensteanbieter könnte sich daher auch nicht auf die Authentizität der Entfernungsanordnung verlassen. Darüber hinaus beinhaltet eine entsprechenden Entfernungsanordnung oft selbst bereits sensible Informationen, etwa in Bezug auf den konkreten Inhalt eines Postings oder der Identität des Betroffenen. Das E-Mail stellt jedoch keinen angemessenen, sicheren Übertragungsweg für derart sensible Informationen dar, weshalb auch die meisten großen Diensteanbieter auf andere Kommunikationskanäle zurückgreifen.

Schließlich widerspricht die Übermittlung per E-Mail auch den Vorgaben in Art. 9 DSA selbst, da dessen Abs. 2 lit. c vorsieht, dass Anordnungen im Sinne des Art. 9 an die von dem Anbieter gemäß Art. 11 benannte elektronische Kontaktstelle geschickt werden müssen, um überhaupt die Pflicht nach Abs. 1 auszulösen. Gemäß Art. 11 Abs. 1 DSA haben Anbieter von Vermittlungsdiensten eine zentrale Kontaktstelle bekannt zu geben, über die sie auf elektronischem Wege unmittelbar mit den

[12] Bundesgesetz, mit dem Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-Netz-Bekämpfungs-Gesetz – HiNBG)

Behörden der Mitgliedstaaten kommunizieren können. Anders als in Bezug auf die zentrale Kontaktstelle für Nutzer iSd Art 12 DSA finden sich in der Verordnung jedoch keine konkreten Vorgaben, welche Art der elektronischen Kommunikation dafür gewählt werden darf. Jedenfalls existiert keine Pflicht, als Kontaktstelle ein E-Mailpostfach anzugeben.

Würde daher der Betroffene wie in § 15 Abs. 1 ECG vorgesehen in Hinkunft zunächst die Übermittlung per E-Mail wählen, würde dies lediglich zu Verzögerungen bis zur tatsächlichen Entfernung der Inhalte führen. Dies kann nicht im Sinn des Gesetzgebers sein. Aus diesem Grund ersucht die ISPA die entsprechende Bestimmung aus dem Entwurf zu streichen bzw. in eventu zumindest im Einklang mit den Vorgaben in Art 9 u. 11 DSA zu ergänzen, dass die Anordnung an die vom Diensteanbieter bekanntgegebene zentrale Kontaktstelle übermittelt werden muss.

Zu § 16 ECG

In § 16 DSA wird eine neue Rechtsgrundlage zur Geltendmachung von immateriellem Schadenersatz bei Ehrenbeleidigungen in einem elektronischen Kommunikationsnetz eingeführt. Die ISPA begrüßt, dass in den Erläuternden Bemerkungen klargestellt wird, dass sich der Schadenersatzanspruch ausschließlich gegen den Verfasser der beleidigenden Nachricht richtet und nicht auch gegen den Anbieter der den Vermittlungsdienst betreibt. Im Gesetzestext selbst wird jedoch nur darauf abgestellt, dass die Person, die den verletzenden Inhalt „bereitgestellt hat“ eine Entschädigung zu leisten hat.

Um Unklarheiten in der Anwendung zu vermeiden, regt die ISPA daher an, die Wortfolge „bereitgestellt hat“ durch „verfasst hat“ zu ersetzen oder in der Bestimmung den folgenden Satz zu ergänzen: „Der Anspruch richtet sich gegen den Verfasser des ehrenbeleidigenden Inhalts und nicht gegen den Vermittlungsdiensteanbieter.“

Zu § 34 KOG

Die ISPA begrüßt ausdrücklich die Neuaufteilung der Finanzierungsbeiträge, da damit der Entwicklung der Tätigkeit der RTR-GmbH Fachbereich Telekom in den vergangenen Jahren entsprochen wird, die in zunehmendem Umfang Aufgaben wahrnimmt, die ausschließlich im öffentlichen Interesse liegen.

Auch die taxative Aufzählung jener Aufgabenbereiche in § 34 Abs. 2a KOG, deren Finanzierung auf den Markt überwälzbar ist, ist ein Schritt in die richtige Richtung. Jedoch ist diese Bestimmung nur dann auch effektiv, wenn die Zuordnung der konkreten Tätigkeiten der Behörde zu den einzelnen Aufgabenbereichen transparent aus dem Budget ersichtlich wird. Aktuell wird im Budget der RTR der finanzielle Gesamtaufwand zwar nach Aufgabenbereichen aufgeschlüsselt dargestellt, es fehlt jedoch jegliche Transparenz, welche Tätigkeiten tatsächlich mit diesen Aufwänden verbunden sind, weshalb Aufwände oftmals nicht nachvollziehbar erscheinen.

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 ersucht daher, dass in § 34 KOG eine weitere Bestimmung aufgenommen wird, mit der die Behörde im Rahmen der jährlichen Budgeterstellung zur konkreten Aufschlüsselung der Tätigkeiten die der Erfüllung der in Abs. 2a genannten Aufgabenbereichen dienen verpflichtet wird, etwa durch Angabe der eingesetzten FTEs.

Zu den Änderungen der Strafprozessordnung (StPO)

Die Neuverortung der bislang in § 76a StPO geregelten Auskunft über Stammdaten bzw. Auskunft über Zugangsdaten in den 5. Abschnitt des 8. Hauptstücks der StPO erscheint grundsätzlich auch aus Sicht der ISPA systemkonform.

Der Wegfall der Voraussetzung, dass diese Ermittlungsmaßnahme zur Aufklärung eines konkreten Verdachts einer Straftat einer bestimmten Person erforderlich ist, ist jedoch kritisch zu hinterfragen. Zwar ist es nachvollziehbar, dass wie in den Erläuternden Bemerkungen angemerkt auch die Ermittlung eines zum Zeitpunkt der Ermittlungsmaßnahme unbekannten Täters ermöglicht werden soll. Dennoch sollte nach Ansicht der ISPA sichergestellt werden, dass durch die Ermittlungsmaßnahme nur Daten des (wenn auch zum Zeitpunkt der Ermittlungsmaßnahme noch unbekannten) Verdächtigen ermittelt werden. Der vorgeschlagene Wortlaut des § 135 Abs. 1a StPO würde es jedoch erlauben, Anbieter zur Auskunft über Name und Adresse zu einer IP-Adresse zu verpflichten, solange diese Daten grundsätzlich zur Aufklärung eines konkreten Tatverdachts erforderlich sein können. Das würde somit auch Daten von Personen miteinschließen, die nicht an der Tatbegehung beteiligt waren, was nach Ansicht der ISPA unverhältnismäßig erscheint.

Die ISPA schlägt daher vor, Anleihen an den Voraussetzungen für eine Anordnung zur Auskunft über Daten einer Nachrichtenübermittlung (Rufdatenrückerfassung) in § 135 Abs. 2 StPO zu nehmen, die gemäß der dazu ergangenen Erläuternden Bemerkungen gerade diese Verhältnismäßigkeit sicherstellen sollen[13] und die Bestimmung wie folgt zu formulieren:

> „(1a) Auskunft über Stammdaten und Auskunft über Zugangsdaten sind zulässig, wenn sie zur Aufklärung eines konkreten Verdachts einer Straftat erforderlich erscheinen und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Verdächtigen ermittelt werden können.

Zu den Änderungen des Auslieferungs- und Rechtshilfegesetzes (ARHG) sowie des Gesetzes über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG)

Die ISPA begrüßt, dass mit den vorgeschlagenen Änderungen die Möglichkeiten zur freiwilligen grenzüberschreitenden Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern erweitert werden sollen. Die freiwillige Auskunft über Nutzerdaten stellt gerade für US-Unternehmen eine bedeutsame Möglichkeit dar, um Strafverfolgungsbehörden in anderen Staaten bei

[13] Vgl EB zu Art II Z 7 der Regierungsvorlage zum Strafrechtsänderungsgesetz 2002

Ermittlungsmaßnahmen zu unterstützen, ohne, dass dafür ein kosten- und zeitintensives Rechtshilfeersuchen verfasst werden muss. Gerade bis zur Umsetzung der Verordnung über Europäische Sicherungs- und Herausgabeanordnungen („E-Evidence Verordnung“)[14] wird diese Art der grenzüberschreitenden Zusammenarbeit weiterhinein eine entscheidende Rolle spielen.

Die Abwicklung der freiwilligen Zusammenarbeit über die Zentrale Abfragestelle für Social Media und Online-Provider (ZASP) als Single Point of Contact für entsprechende Anfragen hat sich in den vergangenen Jahren aus Sicht der betroffenen Diensteanbieter sehr bewährt, und, wie auch ein Blick auf die Erfolgsquote der Anfragen beweist, auch für die Strafverfolgung einen erheblichen Mehrwert gebracht.[15] Die ISPA spricht sich daher dafür aus, dass diese zentrale Anfragestelle auch in Hinkunft bei der Umsetzung der E-Evidence Verordnung eine tragende Rolle zukommt und als SPOC für Anfragen an die betroffenen Online-Plattformen bestehen bleibt.

Da die freiwillige Zusammenarbeit im Rahmen des ARHG sowie des EU-JZGs gemäß dem Novellierungsvorschlags auch auf die Herausgabe von gespeicherten Inhaltsdaten im Rahmen der Sicherstellung (§ 110 StPO) ausgeweitet werden sollen, möchte die ISPA zudem darauf hinweisen, dass Diensteanbieter mit Sitz in den USA, an die der überwiegende Großteil entsprechender Anfragen ergehen wird, aufgrund der gesetzlichen Vorgaben in 18 U.S.C. § 2702, auf freiwilliger Basis grundsätzlich nur „Nicht-Inhaltsdaten“ herausgeben können. Dazu zählen sowohl Stammdaten, als auch Verkehrsdaten. Die Übermittlung von Inhaltsdaten muss hingegen – zumindest bis zum Inkraftreten der E-Evidence Verordnung - grundsätzlich im Rahmen eines Rechtshilfeersuchens angefragt werden.

Wichtig ist es aus Sicht der ISPA schließlich auch bereits frühzeitig der nationalen Umsetzung der E-Evidence Verordnung die notwendige Aufmerksamkeit zu schenken. Dies beinhaltet insbesondere auch die Bereitstellung der notwendigen finanziellen Ressourcen für die Anpassung der in §§ 171ff TKG 2021 geregelten „Durchlaufstelle“, die seit Jahren für den sicheren Datenaustausch zwischen Diensteanbietern und Strafverfolgungsbehörden auf nationaler Ebene sorgt, an die Vorgaben der E-Evidence Verordnung bzw. des darin enthaltenen „dezentralen IT-Systems“ (Art 19 E-EvidenceVO). Denn um die effiziente Zusammenarbeit zwischen Strafverfolgungsbehörden und heimischen Diensteanbietern auch in Zukunft zu gewährleisten ist es essenziell, das Erfolgsmodell der Durchlaufstelle beizubehalten.

Die ISPA hofft auf die Berücksichtigung ihrer Bedenken und Anregungen und steht für Rückfragen und weitere Auskünfte gerne jederzeit zur Verfügung.

[14] Verordnung 2023/1543 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren
[15] Vgl etwa zuletzt Europol SIRIUS EU Digital Evidence Situation Report 2022

Mit freundlichen Grüßen

Mag. Stefan Ebenberger
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

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