



2024-0.884.160-5-A

Bescheid

I. Spruch

Der Antrag der **Atelligo GmbH** (FN 626577 m) vom 02.12.2024 auf Zuerkennung des Status als vertrauenswürdige Hinweisgeberin wird gemäß Art. 22 Abs. 2 der Verordnung (EU) 2022/2065 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, vom 27.10.2022, L 277/56 (DSA) und § 2 Abs. 3 Z 3 des Bundesgesetzes über den Koordinator-für-digitale-Dienste (KDD-G), BGBl. I Nr. 182/2023, abgewiesen.

II. Begründung

1. Gang des Verfahrens

Mit Schreiben vom 02.12.2024 beantragte die Atelligo GmbH (im Folgenden: Antragstellerin) die Zertifizierung als vertrauenswürdiger Hinweisgeber gemäß Art. 22 der Verordnung (EU) 2022/2065 (Digital Services Act, im Folgenden: DSA) für den Bereich der Bekämpfung von Betrug im Online-Bereich, insbesondere Phishing.

Mit Schreiben vom 10.01.2025 ersuchte die KommAustria die Antragstellerin, Angaben und zweckdienliche Unterlagen zum Nachweis der rechtlichen Sachkenntnis gemäß Art. 22 Abs. 2 lit. a DSA, zur organisatorischen Unabhängigkeit von Online-Plattformen gemäß Art. 22 Abs. 2 lit. b DSA, zur bisherigen Erfahrung bei der Meldung von rechtswidrigen Inhalten an Online-Plattformen und den Meldemechanismen gemäß Art. 22 Abs. 2 lit. c DSA sowie Angaben zum Geschäftsmodell der Antragstellerin binnen zwei Wochen nachzureichen.

Die Antragstellerin ist dem Ergänzungsersuchen nicht nachgekommen.

Mit Schreiben vom 17.02.2025 teilte die KommAustria der Antragstellerin unter Hinweis auf die fruchtlos verstrichene Frist zur Ergänzung des Antrags mit, dass erforderliche Nachweise und Unterlagen für die Zertifizierung als vertrauenswürdige Hinweisgeberin nicht erbracht wurden und daher der Antrag abzuweisen sein werde. Zugleich erhielt die Antragstellerin die Möglichkeit sich gemäß § 45 Abs. 3 AVG binnen zwei Wochen zur voraussichtlichen Antragsabweisung zu äußern.

Es langte abermals keine Stellungnahme der Antragstellerin ein.

2. Sachverhalt

Auf Grund des Antrages sowie des durchgeführten Ermittlungsverfahrens steht folgender entscheidungswesentliche Sachverhalt fest:

2.1. Zur Antragstellerin

2.1.1. Rechtsform und Ort der Niederlassung

Die Antragstellerin ist eine zu FN 626577 m beim LG Wiener Neustadt eingetragene Gesellschaft mit beschränkter Haftung. Sie erbringt Dienstleistungen im Bereich IT und Informationssicherheit.

Die Gesellschaft steht zur Hälfte im Eigentum ihres Geschäftsführers A und zur anderen Hälfte in jenem ihres Geschäftsführers B. Das zur Hälfte eingezahlte Stammkapital beträgt EUR XXX. Die Geschäftsführer sind jeweils selbständig vertretungsbefugt.

2.2. Nachweis besonderer Sachkenntnis (Art. 22 Abs. 2 lit. a DSA)

2.2.1. Zur fachlichen Kompetenz in Bezug auf spezifische rechtswidrige Inhalte

Die Antragstellerin erbringt IT-Dienstleistungen zur Bekämpfung von Cyberkriminalität. Der Schwerpunkt der Tätigkeit liegt auf der Entwicklung und Bereitstellung von Softwarelösungen, die darauf abzielen, Unternehmen vor den Gefahren betrügerischer Aktivitäten im Online-Bereich, insbesondere vor Phishing zu schützen und die Sicherheit ihrer Endkunden zu gewährleisten.

Das Team der Antragstellerin besteht vorwiegend aus Cybersicherheitsexperten, die KI-basierte bzw. automatisierte Softwarelösungen (Cybersecurity Software) für Unternehmen entwickeln.

A absolvierte das Studium der angewandten Informatik und verfügt über zahlreiche Zertifizierungen im Sicherheitsbereich (z.B. CISSP, CISM, CCSP, NISG-Prüfer, SPG §55 Stufe „geheim“). B absolvierte das Studium IT-Security und hat ebenfalls diverse Zertifizierungen im Sicherheitsbereich erworben (z.B. IPv6 Security Expert, CCNA, ITIL).

Die Antragstellerin verfügt zwar über Erfahrung in der Cyber-Bedrohungsaufklärung (Threat Intelligence) sowie der automatisierten Erkennung von Phishing, Fake Shops oder Markenverletzungen und ist als Take down Provider, insbesondere für Unternehmen im Bankenumfeld tätig. Zur Identifikation und Beurteilung von rechtswidrigen Inhalten sammelt und analysiert die Antragstellerin Informationen aus öffentlich zugänglichen Quellen (OSINT bzw. Open Source Intelligence). Nähere Angaben dazu wurden nicht gemacht.

Weitere Angaben zur Qualifikation der Angestellten der Antragstellerin hinsichtlich einer juristischen Ausbildung oder spezifischen rechtlichen Expertise besitzen, um rechtswidrige Inhalte als Betrugstatbestände oder überhaupt zweckdienlichen Angaben zu einer spezifischen rechtlichen Expertise der Antragstellerin wurden trotz behördlicher Aufforderungsschreiben nicht gemacht.

2.2.2. Zur Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte

Das Hauptaugenmerk liegt darauf, Unternehmen Softwarelösungen zur Abwehr und Bekämpfung von Cyberkriminalität zur Verfügung zu stellen. Die Antragstellerin besitzt Expertise in der Entwicklung und Bereitstellung von Softwarelösungen zur automatisierten Erkennung und Feststellung von betrügerischen Online-Aktivitäten und kann auf eine mehrjährige Erfahrung bei der Meldung und dem Erwirken der Entfernung betrügerischer Websites gegenüber Internet Service Providern, Webhostern, Content Delivery Networks, Domain Name System Registraren, etc. verweisen. Hierbei handelt es sich jedoch nicht um Online-Plattformen im Sinne des DSA (siehe dazu auch Pkt. 2.4.).

2.3. Nachweis der Unabhängigkeit (Art. 22 Abs. 2 lit. b DSA)

Die Antragstellerin legte in diesem Zusammenhang lediglich dar, ein unabhängiges Unternehmen zu sein. Die Finanzierung des Unternehmens erfolgt durch die beiden Gesellschafter sowie aus der Geschäftstätigkeit, also dem Anbieten von IT-Dienstleistungen zur automatisierten Erkennung von Phishing-Angriffen und weiteren Online-Betrugsformen an Unternehmen.

Zur organisatorischen Unabhängigkeit von Online-Plattformen machte die Antragstellerin trotz behördlicher Aufforderungen keine Angaben.

2.4. Sorgfältige, genaue und objektive Übermittlung von Meldungen (Art. 22 Abs. 2 lit. c DSA)

Die Antragstellerin brachte hierzu vor, dass Phishing oder andere Betrugsversuche entweder automatisch durch selbst entwickelte Erkennungsmaßnahmen oder von Endkunden oder Analysten erfasst und automatisch (falls mit vollständiger Sicherheit feststellbar) bestätigt werden. Im Zuge dessen werden Beweise in Form von Screenshots und weiteren Aufzeichnungen erstellt. Anschließend erfolgen Meldungen automatisch oder manuell an Internet Service Provider, Webhoster, Content Delivery Networks, Domain Name System Registrare und Computer Emergency Response Teams über dafür kommunizierte Kanäle. Alle Kommunikationsschritte werden erfasst und beim jeweiligen Fall mit dokumentiert.

Die Antragstellerin verfügt insofern über mehrjährige Erfahrung in der Übermittlung von Meldungen zur Entfernung entsprechender Websites (Take downs bei Cyberangriffen) im Verhältnis zu Internet Service Providern, Webhostern, Content Delivery Networks, Domain Name System Registraren und Computer Emergency Response Teams.

Die Erfahrung der Antragstellerin bei der Übermittlung von Meldungen bezieht sich damit allerdings auf den Online-Plattformen vorgelagerte Ebenen von Vermittlungsdiensten.

3. Beweiswürdigung

Die Feststellungen ergeben sich aus dem Antrag der Antragstellerin auf Zulassung als vertrauenswürdige Hinweisgeberin. Die festgestellten Beteiligungsverhältnisse beruhen auf dem vorgelegten Firmenbuchauszug.

Die Feststellung, dass die Antragstellerin über die Kompetenz in der Entwicklung und Bereitstellung von Softwarelösungen zur automatisierten Erkennung und Feststellung betrügerischer Online-Aktivitäten, wie Phishing, verfügt, beruht auf den glaubwürdigen Ausführungen im Antrag.

Zu nachfolgenden Anforderungen konnten keine Feststellungen getroffen werden, obwohl In die Behörde in Schreiben vom 10.01.2025 sowie vom 17.02.2025 – über ihr auf ihrer Website verfügbar gemachtes, ausführliches Informationsangebot hinaus – genau die erforderlichen Angaben, die benötigt werden, um den Antrag zu prüfen, dargelegt hat, womit die Mitwirkungspflicht der Antragstellerin ausgelöst wurde, die dieser dann nicht nachgekommen ist (VwGH 22.10.2013, 2012/10/0150):

Mangels Vorlage von Unterlagen konnte nicht festgestellt werden, ob die Antragstellerin über spezifische Fachkompetenz in rechtlicher Hinsicht, insbesondere in der Beurteilung (Erkennen und Feststellen) rechtswidriger Inhalte im Bereich betrugsrechtlicher Tatbestände, etwa Phishing, oder im Bereich des Markenrechts, verfügt. Die angeführte Auswertung von „OSINT“-Quellen (Open Source Intelligence oder Sammlung und Analyse von Informationen aus öffentlich zugänglichen Quellen) stellt keinen Nachweis für rechtliche Sachkenntnis in dem angeführten Rechtsbereich dar.

Zwar wurden zur sorgfältigen, genauen und objektiven Übermittlung von Meldungen an Internet Service Provider, Webhoster, Content Delivery Networks, Domain Name System Registrare und Computer Emergency Response Teams gemacht, die auf den glaubwürdigen Angaben im Antrag beruhen. Es konnten jedoch keine Feststellungen dazu gemacht werden, ob die Antragstellerin über Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte an Online-Plattformen besitzt, da sich die Ausführungen der Antragstellerin lediglich auf ihre Erfahrungen als IT-Dienstleisterin im Verhältnis zu Vermittlungsdiensten bezogen haben, die keine Online-Plattformen im Sinne des DSA sind.

Es konnten schließlich keine Feststellungen zur organisatorischen Unabhängigkeit der Antragstellerin von Online-Plattformen getroffen werden: Die Feststellungen zur Finanzierung der Antragstellerin beruhen auf deren Ausführungen, sich aus ihrer Tätigkeit als Anbieterin von IT-Dienstleistungen zu finanzieren. Die Ausführungen haben sich augenscheinlich aber nicht darauf bezogen, in der beantragten Rolle eines vertrauenswürdigen Hinweisgebers unabhängig von Online-Plattformen zu sein. Ob die Antragstellerin in finanzieller Hinsicht von Online-Plattformen unabhängig ist, konnte daher mangels näherer Angaben nicht beurteilt werden.

4. Rechtliche Beurteilung

4.1. Zur Zuständigkeit der KommAustria als Koordinator für digitale Dienste

Zuständig für die Zuerkennung des Status als vertrauenswürdiger Hinweisgeber ist gemäß Art. 22 Abs. 2 Satz 1 DSA der Koordinator für digitale Dienste des Mitgliedstaates, in dem der Antragsteller niedergelassen ist. Dieser Status ist von allen Anbietern von Online-Plattformen, die in den Anwendungsbereich dieser Verordnung fallen, anzuerkennen (vgl. ErwG 61). Es sind von diesen entsprechende Maßnahmen zu ergreifen, dass die Meldungen der vertrauenswürdigen Hinweisgeber, die über die in Artikel 16 genannten Mechanismen übermittelt werden, vorrangig behandelt und unverzüglich bearbeitet und einer Entscheidung zugeführt werden (Art. 22 Abs. 1 DSA).

Art. 49 Abs. 2 DSA verpflichtet die Mitgliedstaaten, für die Beaufsichtigung der Anbieter von Vermittlungsdiensten und die Durchsetzung dieser Verordnung mindestens eine oder mehrere zuständige Behörden zu benennen. Nach Abs. 2 ist diese bzw. im Fall von mehreren zuständigen Behörden eine dieser Behörden als Koordinator für digitale Dienste zu benennen.

Art. 49 DSA lautet auszugsweise wie folgt:

„Zuständige Behörden und Koordinatoren für digitale Dienste

(1) Die Mitgliedstaaten benennen eine oder mehrere zuständige Behörden, die für die Beaufsichtigung der Anbieter von Vermittlungsdiensten und die Durchsetzung dieser Verordnung zuständig sind (im Folgenden „zuständige Behörden“).

(2) Die Mitgliedstaaten benennen eine der zuständigen Behörden als ihren Koordinator für digitale Dienste. Der Koordinator für digitale Dienste ist für alle Fragen im Zusammenhang mit der Überwachung und Durchsetzung dieser Verordnung in diesem Mitgliedstaat zuständig, es sei denn, der betreffende Mitgliedstaat hat bestimmte besondere Aufgaben oder Sektoren anderen zuständigen Behörden übertragen. Der Koordinator für digitale Dienste ist in jedem Fall dafür zuständig, die Koordinierung dieser Angelegenheiten auf nationaler Ebene sicherzustellen und zu einer wirksamen und einheitlichen Überwachung und Durchsetzung dieser Verordnung in der gesamten Union beizutragen. [...].

[Hervorhebung hinzugefügt]

Gemäß § 2 Abs. 1 KDD-G wurde die nach § 1 des Bundesgesetzes über die Einrichtung einer Kommunikationsbehörde Austria (KOG), BGBl. I Nr. 32/2001 idF BGBl. I Nr. 6/2024, eingerichtete KommAustria mit der Wahrnehmung der Aufgaben des Koordinators für digitale Dienste (KDD) im Sinne des Art. 49 Abs. 1 und 2 DSA beauftragt. Die KommAustria ist gemäß § 10 Abs. 1 KDD-G iVm § 2 Abs. 1 Z 15 KOG Koordinator für digitale Dienste in Österreich und damit für den Antragsteller zuständig, da dessen Sitz sich in Österreich befindet.

4.2. Zum Verfahren der Zuerkennung

Gemäß § 2 Abs. 3 Z 3 KDD-G hat die KommAustria die Zuerkennung des Status als vertrauenswürdiger Hinweisgeber gemäß Art. 22 Abs. 2 DSA mit Bescheid wahrzunehmen.

Das Verfahren der Zuerkennung des Status als vertrauenswürdiger Hinweisgeber folgt den nationalen Verfahrensregeln, soweit der DSA keine abschließenden Regelungen enthält. Die nationalen Verfahrensregeln müssen den rechtsstaatlichen Vorgaben aus Art. 50 Abs. 1 DSA genügen, also unparteiisch und transparent sein und zu zeitnahen Entscheidungen führen (vgl. ErWG 116 zum DSA; Raue in *Hofmann/Raue*, Kommentar zum Digital Services Act, Art. 22 Rn. 46). Die KommAustria hat als Behörde insbesondere das Allgemeine Verwaltungsverfahrensgesetz (AVG) anzuwenden (vgl. dazu auch die Erl zur RV 2309 BlgNR, XXVII. GP zum KDD-G). Daher gelangt für das vorliegende Verfahren das Allgemeine Verwaltungsverfahrensgesetz 1991 (AVG), BGBl. I Nr. BGBl. Nr. 51/1991 idF BGBl. I Nr. 50/2025 zur Anwendung.

In materiellrechtlicher Hinsicht legt wiederum der DSA die Kriterien für die Zuerkennung des Status als vertrauenswürdiger Hinweisgeber fest.

Art. 22 DSA lautet auszugsweise wie folgt:

„Vertrauenswürdige Hinweisgeber

(1) Die Anbieter von Online-Plattformen ergreifen die erforderlichen technischen und organisatorischen Maßnahmen, damit Meldungen, die von in ihrem ausgewiesenen Fachgebiet tätigen vertrauenswürdigen Hinweisgebern über die in Artikel 16 genannten Mechanismen übermittelt werden, vorrangig behandelt und unverzüglich bearbeitet und einer Entscheidung zugeführt werden.

(2) Der Status des vertrauenswürdigen Hinweisgebers nach dieser Verordnung wird auf Antrag einer Stelle vom Koordinator für digitale Dienste des Mitgliedstaats, in dem der Antragsteller niedergelassen ist, einem Antragsteller zuerkannt, der nachgewiesen hat, dass er alle folgenden Bedingungen erfüllt:

- a) die Stelle hat besondere Sachkenntnis und Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte;
- b) sie ist unabhängig von jeglichen Anbietern von Online-Plattformen;
- c) sie übt ihre Tätigkeiten zur Übermittlung von Meldungen sorgfältig, genau und objektiv aus. [...].“

In Erwägungsgrund 61 zum DSA heißt es dazu:

„Abhilfe bei rechtswidrigen Inhalten kann schneller und zuverlässiger erfolgen, wenn Anbieter von Online-Plattformen die erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass von vertrauenswürdigen Hinweisgebern, die innerhalb ihres ausgewiesenen Fachgebiets handeln, im Rahmen der von dieser Verordnung geforderten Melde- und Abhelfemechanismen eingereichte Meldungen vorrangig bearbeitet werden, unbeschadet der Verpflichtung, sämtliche über diese Mechanismen eingereichte Meldungen rasch, sorgfältig und in nicht willkürlicher Weise zu bearbeiten und Entscheidungen dazu zu treffen. Dieser Status des vertrauenswürdigen Hinweisgebers sollte vom Koordinator für digitale Dienste des Mitgliedstaats, in dem der Antragsteller niedergelassen ist, vergeben und von allen Anbietern von Online-Plattformen, die in den Anwendungsbereich dieser Verordnung fallen, anerkannt werden. Dieser Status des vertrauenswürdigen Hinweisgebers sollte nur an Einrichtungen, nicht an Einzelpersonen, vergeben werden, die unter anderem nachgewiesen haben, dass sie über besondere Sachkenntnis und Kompetenz im Umgang mit rechtswidrigen Inhalten verfügen und dass sie ihre Tätigkeit sorgfältig, genau und objektiv durchführen. [...]

Um den Mehrwert eines solchen Verfahrens nicht zu mindern, sollte die Gesamtzahl, der gemäß dieser Verordnung anerkannten vertrauenswürdigen Hinweisgeber begrenzt werden. Insbesondere wird Wirtschaftsverbänden, die die Interessen ihrer Mitglieder vertreten, empfohlen, den Status vertrauenswürdiger Hinweisgeber zu beantragen, unbeschadet des Rechts privater Einrichtungen oder Personen, mit Anbietern von Online-Plattformen bilaterale Vereinbarungen zu schließen.“

[Hervorhebungen hinzugefügt]

Nach dem Wortlaut der deutschen Sprachfassung des Art. 22 DSA (vgl. dazu engl.: *has demonstrated*; franz.: *a démontré*) hat ein Antragsteller darüber hinaus „nachzuweisen“, dass er alle Voraussetzungen des Abs. 2 lit. a bis c erfüllt. Wie streng dieser Nachweis zu führen ist, lässt

die Verordnung allerdings offen (siehe etwa Raue in *Hofmann/Raue*, Kommentar zum Digital Services Act, Art. 22 Rn. 47).

Die Formulierung „Nachweis“ legt im Unterschied zum Begriff der „Glaubhaftmachung“, die lediglich verlangt, dass die Behörde von der Wahrscheinlichkeit – und nicht etwa von der Richtigkeit – des Vorliegens einer bestimmten Tatsache zu überzeugen ist (vgl. VwGH 30.06.2011, 2011/03/0039 zur Vergabe von Hörfunkzulassungen nach dem PrR-G), eine strengere Prüfung der Voraussetzungen nahe. In Zusammenschau mit ErWG 61, der einerseits die Anbieter von Online-Plattformen dazu anhält, die von vertrauenswürdigen Hinweisgebern eingereichten Meldungen vorrangig zu bearbeiten und andererseits den Koordinatoren für digitale Dienste aufträgt, die Gesamtzahl der vertrauenswürdigen Hinweisgeber zu begrenzen, ist somit anzunehmen, dass bei der Prüfung des Vorliegens der Voraussetzungen ein eher strenger Maßstab anzulegen ist (vgl. auch Raue in *Hofmann/Raue*, Kommentar zum Digital Services Act, Art. 22 Rn. 46ff, Rn. 33f).

4.3. Zur Erfüllung der Antragsvoraussetzungen

Der Wortlaut des Art. 22 Abs. 2 DSA verlangt einerseits, dass ein Nachweis für das Vorliegen der Voraussetzungen gemäß lit. a bis c erbracht werden muss und andererseits, dass alle Voraussetzungen für die Zuerkennung des Status als vertrauenswürdiger Hinweisgeber erfüllt sein müssen (arg. „*Der Status des vertrauenswürdigen Hinweisgebers [...] zuerkannt, der nachgewiesen hat, dass er alle folgenden Bedingungen erfüllt: ...*“), widrigenfalls eine Zuerkennung zu versagen ist. Die bloße Behauptung, wonach sie über die Kompetenz der Erkennung rechtswidriger Inhalte verfügt, reicht hierbei nicht aus (arg: *Nachweis*).

Nach Art. 22 Abs. 2 lit. a DSA muss die Einrichtung, die den Status als vertrauenswürdiger Hinweisgeber beantragt, über besondere Sachkenntnis und Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte verfügen. Hintergrund für das Erfordernis einer besonderen Sachkenntnis und Kompetenz im Umgang mit rechtswidrigen Inhalten ist einerseits – wie schon zum Verfahren im Allgemeinen dargelegt wurde – die mit der Einrichtung der vertrauenswürdigen Hinweisgeber einhergehende Verpflichtung der Online-Plattformen, deren Meldungen vorrangig zu behandeln und andererseits das Ziel der Verfahrensbeschleunigung (vgl. dazu ausführlich Nägele/Dilbaz in *Müller-Terpitz/Köhler*, Kommentar zum Digital Services Act, Art. 22 Rn. 32ff).

Im Regelfall muss daher die antragstellende Einrichtung über entsprechend qualifiziertes Personal in dem spezifischen Rechtsgebiet verfügen, um diese in die Lage zu versetzen, rechtswidrige Informationen zu erkennen bzw. festzustellen. Es geht daher bei der spezifischen Sachkenntnis vor allem, wenngleich nicht nur, um die erforderlichen juristischen Fachkenntnisse.

Schließlich muss die Organisation fähig sein, sorgfältige, genaue und objektive Meldungen an Online-Plattformen verfassen zu können. Diese Kompetenz im Umgang mit rechtswidrigen Inhalten kann (im Idealfall) durch praktische Erfahrungen in der Vergangenheit, etwa erfolgreich durchgeführte Beschwerdeverfahren mit Online-Plattformen, belegt werden (vgl. Raue in *Hofmann/Raue*, Kommentar zum Digital Services Act, Art. 22 Rn. 41). Für Einrichtungen, die noch keine einschlägige Erfahrung in der Meldung rechtswidriger Inhalte an Online-Plattformen haben, könnten etwa Musterprozesse dargelegt werden oder könnte ein hinreichend detailliertes Konzept über den beabsichtigten Meldemechanismus als Nachweis dienen.

4.3.1. Zum Nachweis besonderer Sachkenntnis (lit. a)

Gemäß Art. 3 lit. h DSA handelt es sich bei „rechtswidrigen Inhalten“ um alle Informationen, die als solche oder durch ihre Bezugnahme auf eine Tätigkeit, einschließlich des Verkaufs von Produkten oder der Erbringung von Dienstleistungen, nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen, ungeachtet des genauen Gegenstands oder der Art der betreffenden Rechtsvorschriften. Erwägungsgrund 12 zum DSA führt im Hinblick auf den Begriff „rechtswidrige Inhalte“ insbesondere Nachstehendes aus:

„Um das Ziel zu erreichen, ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld sicherzustellen, sollte die Definition des Begriffs „rechtswidrige Inhalte“ für die Zwecke dieser Verordnung im Großen und Ganzen den bestehenden Regeln in der Offline-Umgebung entsprechen. Insbesondere sollte der Begriff „rechtswidrige Inhalte“ so weit gefasst werden, dass er Informationen im Zusammenhang mit rechtswidrigen Inhalten, Produkten, Dienstleistungen oder Tätigkeiten umfasst. Insbesondere sollte der Begriff so ausgelegt werden, dass er sich auf Informationen unabhängig von ihrer Form bezieht, die nach geltendem Recht entweder an sich rechtswidrig sind, etwa rechtswidrige Hassrede, terroristische Inhalte oder rechtswidrige diskriminierende Inhalte, oder nach dem geltenden Recht rechtswidrig sind, weil sie mit rechtswidrigen Handlungen zusammenhängen. Beispiele hierfür sind etwa die Weitergabe von Darstellungen sexuellen Missbrauchs von Kindern, die rechtswidrige Weitergabe privater Bilder ohne Zustimmung, Cyber-Stalking, der Verkauf nicht konformer oder gefälschter Produkte, der Verkauf von Produkten oder die Erbringung von Dienstleistungen unter Verstoß gegen das Verbraucherschutzrecht, die nicht genehmigte Verwendung urheberrechtlich geschützten Materials, das rechtswidrige Angebot von Beherbergungsdienstleistungen oder der rechtswidrige Verkauf von lebenden Tieren. [...]“

Dies bedeutet, dass jeder Inhalt, der in einem konkreten Fall in Widerspruch zu Rechtsvorschriften steht, rechtswidrig ist. Diese Rechtsvorschriften können sowohl dem nationalen als auch dem europäischen Recht entspringen. Der Begriff des rechtswidrigen Inhalts ist also weit zu verstehen und umfasst nicht allein rechtswidrige Inhalte, sondern auch rechtswidrige Tätigkeiten (z.B. die Erbringung von Dienstleistungen unter Verstoß gegen das Verbraucherschutzrecht). Zentrales Anliegen des DSA bleibt dabei die Bekämpfung von rechtswidrigen Inhalten im Online-Umfeld (dazu umfassend Hofmann in *Hofmann/Raue*, Kommentar zum Digital Services Act, Art. 3 lit. h Rn. 71ff).

Wie sich darüber hinaus aus dem Wortlaut des Art. 22 DSA ergibt, sind die Aufgaben vertrauenswürdiger Hinweisgeber in Zusammenhang mit den für Online-Plattformen gemäß Art. 3 lit. i DSA normierten Sorgfaltspflichten in Abschnitt 3 zu sehen. Für Vermittlungsdienste auf vorgelagerten Ebenen besteht insoweit nämlich keine Pflicht, *„technische und organisatorische Maßnahmen zu ergreifen, damit Meldungen, die von in ihrem ausgewiesenen Fachgebiet tätigen vertrauenswürdigen Hinweisgebern über die in Artikel 16 genannten Mechanismen übermittelt werden, vorrangig behandelt und unverzüglich bearbeitet und einer Entscheidung zugeführt werden können“*.

Zum Nachweis ihrer spezifischen Sachkenntnis und Kompetenz zur Erkennung, Feststellung und Meldung rechtswidriger Online-Inhalte verwies die Antragstellerin einerseits auf ihre mehrjährige Erfahrung bei der Entwicklung und Bereitstellung KI-gestützter bzw. automatisierter Softwarelösungen zur Erkennung und Abwehr verschiedener betrügerischer Online-Aktivitäten und andererseits auf ihre Erfahrung als sogenannter „Take down Provider“ bei der Entfernung entsprechender Inhalte bzw. Websites im Verhältnis zu Internet Service Providern, Webhostern,

Content Delivery Networks, Domain Name System Registraren und Computer Emergency Response Teams.

Es bestehen seitens der Behörde zwar keine Bedenken, dass die Antragstellerin Expertise in der Entwicklung von Softwarelösungen zur automatisierten Erkennung und Bekämpfung betrügerischer Online-Aktivitäten besitzt. Die Zuerkennung des Status als vertrauenswürdige Hinweisgeberin hätte jedoch erfordert, die einschlägigen rechtlichen Kenntnisse im angegebenen Rechtsgebiet – vor allem jene der im Bereich des Betrugs einschlägigen Rechtsgrundlagen – darzulegen. Vorbringen dazu, ob und welche Mitarbeitende über eine juristische Ausbildung und spezifische rechtliche Expertise in dem angegebenen Rechtsgebiet verfügen, erstattete die Antragstellerin allerdings nicht. Hinzu kommt, dass die Antragstellerin ausschließlich auf konkrete Erfahrungen in der Erwirkung von Entfernungen (Take downs) betrügerischer Online-Inhalte (Websites) im Verhältnis zu solchen Vermittlungsdiensten verwiesen hat, die als reine „Durchleitungs- und Caching-Dienste“ im Sinne des DSA zu qualifizieren sind. Wie eingangs erwähnt, setzt die Zuerkennung des Status als vertrauenswürdige Hinweisgeberin auch die Kompetenz voraus, Meldungen rechtswidriger Inhalte an Online-Plattformen zu übermitteln.

Da im Lichte des Art. 22 Abs. 2 lit. a DSA wesentliche Fragen unbeantwortet blieben, ist der Antragstellerin der Nachweis der besonderen Sachkenntnis und der Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte nicht gelungen.

4.3.2. Zum Nachweis der Unabhängigkeit gemäß Art. 22 Abs. 2 lit. b DSA

Die im Zulassungsverfahren zu prüfende Unabhängigkeit zielt auf die Unabhängigkeit der vertrauenswürdigen Hinweisgeber gegenüber Online-Plattformen ab. Es ist damit nicht allein die finanzielle Unabhängigkeit, sondern auch die organisatorische und personelle gemeint. Die Antragstellerin hat keinerlei Nachweise zur Erfüllung des Unabhängigkeitskriteriums hinsichtlich allfälliger Beziehungen zu Online-Plattformen vorgelegt und wurden diese auch trotz Aufforderung nicht nachgereicht.

Eine Prüfung der Bezug habenden Voraussetzungen konnte somit nicht erfolgen und ist daraus zu schließen, dass mangels diesbezüglicher Ausführungen der Nachweis über die Unabhängigkeit von jeglichen Anbietern von Online-Plattformen nicht gelungen ist.

4.3.3. Zur sorgfältigen, genauen und objektiven Ausübung der Tätigkeit der Übermittlung von Meldungen gemäß Art. 22 Abs. 2 lit. c DSA

Die Einrichtung, der der Status als vertrauenswürdiger Hinweisgeber zuerkannt wird, muss in der Lage sein, Meldungen sorgfältig, präzise und objektiv zu übermitteln. Ein solcher Beleg kann etwa dadurch erfolgen, dass über diesbezügliche, konkrete Erfahrungen in der Vergangenheit Ausführungen gemacht werden, oder (bzw. und) dargelegt wird, wie die Meldungstätigkeit konkret von statten gehen soll. Die Einrichtung, der der Status als vertrauenswürdiger Hinweisgeber zuerkannt wird, muss in der Lage sein, Meldungen sorgfältig, präzise und objektiv zu übermitteln. Ein solcher Beleg kann etwa dadurch erfolgen, dass über diesbezügliche, konkrete Erfahrungen in der Vergangenheit Ausführungen gemacht werden, oder (bzw. und) dargelegt wird, wie die Meldungstätigkeit konkret von statten gehen soll.

Die Antragstellerin brachte hierzu vor, dass Phishing oder andere Betrugsversuche entweder automatisch durch selbst entwickelte Erkennungsmaßnahmen oder von Endkunden oder Analysten erfasst und automatisch (falls mit vollständiger Sicherheit feststellbar) bestätigt werden. Im Zuge dessen werden Beweise in Form von Screenshots und weiteren Aufzeichnungen erstellt. Anschließend erfolgen Meldungen automatisch oder manuell an Internet Service Provider, Webhoster, Content Delivery Networks, Domain Name System Registrare und Computer Emergency Response Teams über dafür kommunizierte Kanäle. Alle Kommunikationsschritte werden erfasst und beim jeweiligen Fall mit dokumentiert.

Die Antragstellerin verfügt insofern über mehrjährige Erfahrung in der Übermittlung von Meldungen zur Entfernung entsprechender Websites (Take downs bei Cyberangriffen) im Verhältnis zu Internet Service Providern, Webhostern, Content Delivery Networks, Domain Name System Registraren und Computer Emergency Response Teams.

Die Erfahrung der Antragstellerin bei der Übermittlung von Meldungen bezieht sich damit allerdings auf den Online-Plattformen vorgelagerte Ebenen von Vermittlungsdiensten, nicht jedoch auf erstere. Art. 22 DSA bezieht die institutionalisierte Rolle von vertrauenswürdigen Hinweisgebern jedoch nur auf Online-Plattformen. Damit wurden, dies auch vor dem Hintergrund behördlicher Aufforderungsschreiben, sich auf Online-Plattformen beziehende Erfahrungen betreffend die genaue, objektive und sorgfältige Übermittlungen von Meldungen nicht dargelegt.

Zusammenfassend ist daher davon auszugehen, dass der Antragstellerin – auch – mangels näherer Ausführungen bzw. Belege der Nachweis über das Vorliegen der Voraussetzungen für die Zuerkennung des Status als vertrauenswürdiger Hinweisgeber gemäß Art. 22 Abs. 2 DSA nicht gelungen ist, dass sie nämlich über besondere Sachkenntnis und Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte verfügt, dass sie unabhängig von Online-Plattformen ist und die sorgfältige, genaue und objektive Übermittlung von Meldungen entfallen wird, zumal sämtliche Voraussetzungen für die Zuerkennung des Status als vertrauenswürdige Hinweisgeberin kumulativ erfüllt sein müssen.

Es war daher spruchgemäß zu entscheiden.

III. Rechtsmittelbelehrung

Gegen diesen Bescheid steht der/den Partei/en dieses Verfahrens das Rechtsmittel der Beschwerde gemäß Art. 130 Abs. 1 Z 1 B-VG beim Bundesverwaltungsgericht offen. Die Beschwerde ist binnen vier Wochen nach Zustellung dieses Bescheides schriftlich, telegraphisch, fernschriftlich, im Wege automationsunterstützter Datenübertragung oder in jeder anderen technisch möglichen Weise bei der Kommunikationsbehörde Austria einzubringen. Die Beschwerde hat den Bescheid, gegen den sie sich richtet, ebenso wie die belangte Behörde, die den Bescheid erlassen hat, zu bezeichnen und die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt, das Begehren sowie die Angaben zu enthalten, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht wurde.

Für die Beschwerde ist eine Gebühr in Höhe von EUR 50,- an das Finanzamt Österreich (IBAN: AT830100000005504109, BIC: BUNDATWW, Verwendungszweck: „Bundesverwaltungsgericht / GZ 2024-0.884.160-5-A“, Vermerk: „Name des Beschwerdeführers“) zu entrichten. Bei elektronischer Überweisung der Beschwerdegebühr mit der „Finanzamtszahlung“ sind die Steuernummer/Abgabenkontonummer 109999102, die Abgabenart „EEE – Beschwerdegebühr“, das Datum des Bescheides als Zeitraum und der Betrag anzugeben. Die Entrichtung der Gebühr ist durch einen Zahlungsbeleg oder einen Ausdruck über die erfolgte Erteilung einer Zahlungsanweisung nachzuweisen.

Wien, am 31.10.2025

Kommunikationsbehörde Austria

Mag.Dr. Susanne Lackner
(Vorsitzende-Stellvertreterin)