KommAustria
Kommunikationsbehörde Austria

Artikel 22 DSA Vertrauenswürdige Hinweisgeber „Trusted Flaggers“

Information für Antragstellende

Veröffentlichung: 12 März 2024

Kommunikationsbehörde Austria (KommAustria)
Mariahilfer Straße 77–79
1060 WIEN, ÖSTERREICH
www.rtr.at
E: rtr@rtr.at
T: +43 1 58058-0
F: +43 1 58058-9191

Vorbemerkung

Gegenständliches Merkblatt erläutert die Voraussetzungen für die Erlangung einer Zertifizierung zum Trusted Flagger („Vertrauenswürdiger Hinweisgeber“) gemäß Art. 22 Digital Services Act (DSA) in Verbindung mit § 2 Abs. 3 Z 3 Koordinator-für-Digitale-Dienste-Gesetz (KDD-G) durch die KommAustria. Die Unterlage wurde zur Orientierung von Antragstellenden in Abstimmung mit den Koordinatoren für digitale Dienste anderer EU-Mitgliedstaaten erstellt, um eine möglichst abgestimmte, EU-weit vergleichbare Auslegung der Bezug habenden Bestimmungen zu ermöglichen.

Diese Anleitung ist nicht verbindlich, dient jedoch der Erläuterung. Einzig maßgeblich in rechtlicher Hinsicht sind die Bestimmungen über Trusted Flaggers insbesondere in Art. 22 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 (Gesetz über digitale Dienste, „Digital Services Act“, „DSA“). Etwaige von der Europäischen Kommission erst zu erlassende Leitlinien nach Art. 22 Abs. 8 DSA wirken sich nicht rückwirkend auf abgeschlossene Verfahren zur Zertifizierung als Trusted Flagger aus. Darüber hinaus ist zu berücksichtigen, dass jede Zertifizierung eine Einzelfallentscheidung auf der Grundlage der in Art. 22 Abs. 2 DSA verankerten Kriterien darstellt, auf das Verfahren selbst kommt das AVG zur Anwendung.

1 Was sind Trusted Flaggers?

Dies sind Einrichtungen mit spezifischen Fachkenntnissen und Kompetenzen, deren Meldungen über rechtswidrige Inhalte bei Online-Plattformen privilegiert behandelt werden müssen, was allerdings nicht mit der Pflicht zur Entfernung des betreffenden Inhalts gleichzusetzen ist. Online-Plattformen haben schon bisher auf freiwilliger Basis Einrichtungen privilegierten Flagger-Status eingeräumt. Neu ist im Rahmen von Artikel 22 DSA, dass sich Einrichtungen von Koordinatoren für digitale Dienste **als Trusted Flaggers zur Meldung rechtswidriger Inhalte zertifizieren lassen können, und als solche zwingend von allen Online-Plattformen anzuerkennen sind.** Diese müssen Maßnahmen ergreifen, um sicherzustellen, dass die von Trusted Flaggern eingereichten Meldungen vorrangig behandelt, unverzüglich bearbeitet und entschieden werden. Diese Maßnahmen sind für die Plattformen verbindlich und eine **Nicht-Einhaltung kann vom Koordinator für digitale Dienste sanktioniert** werden. Zertifizierte Trusted Flaggers können grundsätzlich **EU-weit tätig** werden. Unter bestimmten Umständen kann der Status des Trusted Flagger vom zuständigen Koordinator für digitale Dienste widerrufen werden. Durch die Zertifizierung entsteht für den Trusted Flagger die Verpflichtung, jährlich Transparenzberichte über die erstatteten Meldungen zu erstellen.

Durch den besonderen Status des Trusted Flagger normiert der DSA einen allgemeinen Auftrag an die Koordinatoren für digitale Dienste, nicht eine zu große Anzahl an Trusted Flaggers zuzulassen. Dies präjudiziert in keinem Fall bestimmte Anträge, dennoch besteht das Ziel, das Spektrum typischer rechtswidriger Inhalte durch spezialisierte Trusted Flaggers im jeweiligen Mitgliedstaat abzudecken.

Justiz- und Verwaltungsbehörden stehen Anordnungen gegen illegale Inhalte im Sinne des Art. 9 DSA und zusätzliche materiell-rechtliche Ermächtigungen zur Verfügung, mit denen sie gegen inkriminierte Inhalte vorgehen können. Es liegt daher grundsätzlich nahe, die Rolle des Trusted Flagger an jene Antragstellende zu vergeben, die keine anderen direkten und vorrangigen Mittel haben, um Inhalte auf Online-Plattformen zu melden.

Von besonderer Bedeutung für den Status des Trusted Flaggers ist die Unabhängigkeit, insbesondere im Hinblick auf allfällige Verbindungen zu Online-Plattformen. Ebenso wichtig ist Transparenz, einschließlich jene des Zertifizierungsprozesses. Dementsprechend hat die Europäische Kommission gemäß Art. 22 Abs. 5 DSA ein öffentliches Register aller zertifizierten Trusted Flaggers zu erstellen.

Die Bestimmungen hinsichtlich zertifizierter Trusted Flaggers gelten – wie der DSA selbst – für alle Arten rechtswidriger Inhalte. Dies umfasst naturgemäß ein weites Feld, der DSA selbst zitiert daher (wenngleich keineswegs in abschließender Weise) typischerweise vorkommende rechtswidrige Inhalte.

In Erwägungsgrund 12 DSA heißt es etwa:

„*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. Im Gegensatz dazu sollte ein Augenzeugenvideo eines potenziellen Verbrechens nicht als rechtswidriger Inhalt betrachtet werden, nur weil es eine*

rechtswidrige Handlung zeigt, wenn die Aufnahme oder öffentliche Verbreitung eines solchen Videos nach nationalem Recht oder Unionsrecht nicht rechtswidrig ist. In dieser Hinsicht ist es unerheblich, ob die Rechtswidrigkeit der Information oder der Handlung sich aus dem Unionsrecht oder aus mit dem Unionsrecht im Einklang stehendem nationalem Recht ergibt, um welche Art von Rechtsvorschriften es geht und was diese zum Gegenstand haben." (Hervorhebung hinzugefügt)

2 Voraussetzungen für die Zertifizierung

Gemäß Art. 22 Abs. 2 DSA müssen Trusted Flaggers, die eine Zertifizierung durch die Behörde anstreben, folgende Voraussetzungen mitbringen:

- Die betreffende Einrichtung muss über besondere Sachkenntnis und Kompetenz in Bezug auf die Erkennung, Feststellung und Meldung rechtswidriger Inhalte verfügen
- Sie muss unabhängig von jeglichen Anbietern von Online-Plattformen sein
- Sie muss ihre Tätigkeiten zur Übermittlung von Meldungen sorgfältig, genau und objektiv ausfüllen

Zur Auslegung der Begriffe „Sachkenntnis und Kompetenz" und „sorgfältige, genaue und objektive" Tätigkeit erfolgen nachfolgend einige Erläuterungen.

Erwägungsgrund 61 DSA besagt:

„...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…" (Hervorhebung hinzugefügt)

Bei der Beurteilung des Nachweises der „Sachkenntnis und Kompetenz" können insbesondere folgende Aspekte eine Rolle spielen:

- Sachkenntnis bei der Aufdeckung und Bekämpfung rechtswidriger Online-Inhalte, insbesondere juristische Sachkenntnis (in Bezug auf das einschlägige Unionsrecht sowie die nationalen Rechtsvorschriften der Mitgliedstaaten, in denen Antragstellende tätig sind bzw. tätig zu werden beabsichtigen)
- Fachkenntnis (etwa in Bezug auf die Aufdeckung des Verkaufs von Fälschungen und/oder der Nichtkonformität von Produkten) in Bezug auf verschiedene Arten rechtswidriger Inhalte. Wie in Erwägungsgrund 61 DSA dargelegt, sollten die zertifizierten Trusted Flaggers in Anbetracht des breiten Spektrums rechtswidriger Inhalte zwar in dem ihnen zugewiesenen Fachgebiet tätig werden, dies kann allerdings mehrere Arten rechtswidriger Inhalte abdecken

- Kompetenz im Bereich der Nutzung digitaler Technologien, insbesondere bei der Beobachtung von Online-Plattformen und bei der Meldung potenziell rechtswidriger Inhalte (Fachwissen des Personals und einschlägige Berufserfahrung), einschließlich spezifischer Erfahrung im Melden (Flagging oder auch „Notifying“)
- Rechtliches Fachwissen und Fachkenntnisse bei der Aufdeckung und Bekämpfung rechtswidriger Online-Inhalte können durch für neue Mitarbeitende zur Verfügung gestellten Schulungs- und Bewertungsinstrumente nachgewiesen werden
- Sachkenntnis (allenfalls auch durch Beiziehung von externen Beratenden), wenn die zu bewertenden Inhalte spezifisch wissenschaftlicher Natur sind (z.B. Produkte mit Inhaltsstoffen, deren Verkauf aufgrund von Gesundheitsrisiken verboten ist)
- Engagement für die Sicherheit der Nutzenden, die Achtung ihrer Rechte in Bezug auf rechtswidrige Inhalte und (wenn es um die Kennzeichnung von Inhalten geht) ihrer Grundrechte, einschließlich u. a. des Rechts auf freie Meinungsäußerung und Informationsfreiheit
- Ausreichende personelle und technische und/oder finanzielle Ressourcen, um gegebenenfalls Inhalte regelmäßig zu melden (z.B. Mechanismus auf eigenen Websites, über den Dritte ein Problem melden können oder Verfahren oder Instrumente zur proaktiven Aufdeckung/Verfolgung rechtswidriger Inhalte)

3 Antragsunterlagen

Zunächst ist ein Antrag an die KommAustria auf Zuerkennung des Status eines Trusted Flagger zu stellen, dies kann formlos oder über das verfügbare Antragsformular auf unserer Webseite erfolgen.

Wir empfehlen zur Vermeidung von Nachforderungen einem Antrag insbesondere nachstehende Nachweise beizulegen, wobei grundsätzlich alles beigelegt werden kann bzw. sollte, was für die Antragstellung relevant sein könnte. Weiters ist beachtlich, dass die empfohlenen Nachweise sich auch auf Erfahrungen mit rechtswidrigen Vorgängen außerhalb des Online-Umfelds beziehen können (etwa besondere Erfahrung in der Opferschutzbegleitung, Menschenrechtsorganisationen, u. ä.). So es sich um eine junge/neue Organisation handelt, sind die entsprechenden Vorhaben ebenso detailliert anzugeben.

3.1 Allgemeine Angaben:

- Genaue Bezeichnung der Organisation/Entität
- einschließlich Vorlage der Statuten bzw. Gründungsakt, bei Unternehmen Firmenbuchauszug
- Angaben zum Firmensitz
- Identitätsnachweise von Vorständen/Geschäftsführenden

- Erläuterungen über die Zielsetzung der Einrichtung und der bisherigen Arbeitsweise

3.2 Angaben zur Unabhängigkeit

3.2.1 Organisatorische Unabhängigkeit

Darlegungen über deren Sicherstellung (interne Richtlinien, Unvereinbarkeiten/Interessenskonflikte, Vereinbarungen mit Plattformen, u. ä…)

3.2.2 Finanzierung und finanzielle Unabhängigkeit

Darlegungen zur Finanzierung: Vollständige Offenlegung bzw. Aufschlüsselung der Finanzierungsquellen (allenfalls Vorlage von Jahresabschlüssen o.ä.); bei Finanzierung durch Plattformen eidesstattliche Erklärung der Geschäftsführung/des Vorstandes, dass daran keine die Unabhängigkeit beeinträchtigenden Bedingungen geknüpft sind sowie Vorlagen der Finanzierungsvereinbarungen mit der/n Plattformen

3.3 Angaben zu Sachkenntnis und Kompetenz: Erkennen, Identifizieren und Melden rechtswidriger Inhalte (beispielhafte Aufzählung)

- Frühere Jahresberichte, die eine besondere Expertise im Bereich bestimmter rechtswidriger Inhalte belegen
- Vorlage von Zahlen und Statistiken, die die Zahl der Meldungen, geordnet nach Art der rechtswidrigen Inhalte belegen sowie Angaben über die Plattformen, bei denen bisher gemeldet wurde (einschließlich der gewonnenen Erfahrungen)
- Ausführungen hinsichtlich der Maßnahmen, die bei Auffinden rechtswidriger Inhalte ergriffen wurden, einschließlich geübter Praxis bei Nachfragen bei Plattformen, wenn gemeldete Inhalte nicht gelöscht werden; allenfalls Praxis der Weiterleitung an zuständige Behörden (Polizei, Staatsanwaltschaften, etc…)
- Beratungsmaßnahmen für Betroffene
- Frühere Veröffentlichungen, Studien, Beiträge, Kommunikationsmaßnahmen
- Lebensläufe von Mitarbeitenden mit besonderem Fokus auf deren fachliche Qualifikation in Bezug auf die Art der zu meldenden Inhalte; insbesondere auch im Zusammenhang relevante IT-Kenntnisse sowie vorhandene Sprachkenntnisse (vor allem wenn geplant ist, in anderen Mitgliedstaaten tätig zu werden), Schulungsmaßnahmen
- Auskunft über vorhandene juristische Expertise (einschließlich Aus- bzw. Weiterbildung) bzw. externen Rechtsbeistand sowie Darstellung, wie juristische Einschätzung durch Mitarbeitende vorgenommen wird
- Darstellung der Methodik, die zur Erkennung, Identifizierung und Meldung rechtswidriger Inhalte verwendet wird

- Darstellung der Vorgehensweise bei der Sicherung von Beweisquellen
- Interne Qualitätssicherungsmaßnahmen

4 Antragskosten

Im Fall der Erteilung einer Zertifizierung ist eine Bundesverwaltungsabgabe in der Höhe von 6,50 - Euro binnen 14 Tagen nach Erteilung der Zertifizierung zu entrichten (TP 1 der Bundesverwaltungsabgabenverordnung).

5 Anhang

5.1 Relevante Bestimmungen des DSA

Erwägungsgrund (61):

„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 Abhilfemechanismen 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. Es kann sich dabei um öffentliche Einrichtungen handeln, bei terroristischen Inhalten etwa die Meldestellen für Internetinhalte der nationalen Strafverfolgungsbehörden oder der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), oder um Nichtregierungsorganisationen und private oder halböffentliche Einrichtungen wie Organisationen, die Teil des INHOPE-Meldestellennetzes zur Meldung von Material über sexuellen Kindesmissbrauch sind, oder Organisationen für die Meldung rechtswidriger rassistischer und fremdenfeindlicher Darstellungen im Internet. 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.“

Erwägungsgrund (62):

„Vertrauenswürdige Hinweisgeber sollten leicht verständliche und ausführliche Berichte über gemäß dieser Verordnung erfolgte Meldungen veröffentlichen. In diesen Berichten sollten Informationen wie die Anzahl der vom Anbieter von Hostingdiensten kategorisierten Meldungen, die Art der Inhalte und die vom Anbieter ergriffenen Maßnahmen genannt werden. Da vertrauenswürdige Hinweisgeber über Sachkenntnis und Kompetenz verfügen, kann davon ausgegangen werden, dass die von ihnen eingereichten Meldungen mit weniger Aufwand und daher schneller bearbeitet werden können als die von anderen Nutzern eingereichten Meldungen. Die durchschnittliche Bearbeitungsdauer kann jedoch unter anderem je nach Art der rechtswidrigen Inhalte, der Qualität der Meldungen und den für die Einreichung solcher Meldungen geltenden technischen Verfahren variieren.

Während beispielsweise im Verhaltenskodex für die Bekämpfung rechtswidriger Hassreden im Internet von 2016 für die teilnehmenden Unternehmen ein Richtwert für die Zeit festgelegt wird, die für die Bearbeitung gültiger Meldungen im Hinblick auf die Entfernung rechtswidriger Hassreden benötigt wird, können die Bearbeitungsfristen für andere Arten rechtswidriger Inhalte je nach den spezifischen Tatsachen und Umständen und der Art der betreffenden rechtswidrigen Inhalte erheblich variieren. Damit der Status eines vertrauenswürdigen Hinweisgebers nicht missbräuchlich verwendet wird, sollte es möglich sein, diesen Status auszusetzen, wenn ein Koordinator für digitale Dienste am Niederlassungsort aus berechtigten Gründen eine Untersuchung eingeleitet hat. Die Vorschriften dieser Verordnung in Bezug auf vertrauenswürdige Hinweisgeber sollten nicht so ausgelegt werden, dass sie die Anbieter von Online-Plattformen daran hindern, Meldungen von Einrichtungen oder Einzelpersonen ohne den Status eines vertrauenswürdigen Hinweisgebers im Sinne dieser Verordnung auf ähnliche Weise zu behandeln oder im Einklang mit dem geltenden Recht, einschließlich dieser Verordnung und der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates(29), auf andere Art mit weiteren Einrichtungen zusammenzuarbeiten. Die Bestimmungen dieser Verordnung sollten die Anbieter von Online-Plattformen nicht daran hindern, solche vertrauenswürdigen Hinweisgeber oder ähnliche Verfahren zu nutzen, um rasch und zuverlässig gegen Inhalte vorzugehen, die mit ihren allgemeinen Geschäftsbedingungen unvereinbar sind, insbesondere gegen Inhalte, die schutzbedürftigen Nutzern, wie etwa Minderjährigen, schaden.“

Erwägungsgrund (87):

„Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen sollten im Rahmen solcher Risikominderungsmaßnahmen beispielsweise in Betracht ziehen, die erforderliche Gestaltung, Funktion oder Funktionsweise ihres Dienstes, wie etwa die Gestaltung der Online-Schnittstelle, anzupassen. Sie sollten ihre allgemeinen Geschäftsbedingungen nach Bedarf und im Einklang mit den Bestimmungen dieser Verordnung über die allgemeinen Geschäftsbedingungen anpassen und anwenden. Weitere geeignete Maßnahmen könnten die Anpassung ihrer Systeme und internen Verfahren zur Moderation von Inhalten oder die Anpassung ihrer Entscheidungsprozesse und Ressourcen, einschließlich des Personals für die Moderation von Inhalten, seiner Ausbildung und seines lokalen Fachwissens, umfassen. Dies betrifft insbesondere die Geschwindigkeit und Qualität der Bearbeitung von

Meldungen. In diesem Zusammenhang wird beispielsweise im Verhaltenskodex für die Bekämpfung rechtswidriger Hassreden im Internet aus dem Jahr 2016 ein Referenzwert für die Bearbeitung gültiger Meldungen über die Entfernung rechtswidriger Hassreden von weniger als 24 Stunden festgelegt. Anbieter sehr großer Online-Plattformen, insbesondere solcher, die in erster Linie für die öffentliche Verbreitung pornografischer Inhalte genutzt werden, sollten all ihren Verpflichtungen aus dieser Verordnung in Bezug auf rechtswidrige Inhalte, die Gewalt im Internet darstellen, einschließlich rechtswidriger pornografischer Inhalte, sorgfältig nachkommen, insbesondere im Hinblick darauf, dass Opfer ihre Rechte in Bezug auf Inhalte, die die nicht einvernehmliche Weitergabe von intimem oder manipuliertem Material darstellen, durch die rasche Bearbeitung von Meldungen und die Entfernung solcher Inhalte unverzüglich wirksam ausüben können. Für andere Arten rechtswidriger Inhalte können abhängig von den Fakten, Umständen und Arten der betreffenden rechtswidrigen Inhalte längere oder kürzere Fristen für die Bearbeitung von Meldungen erforderlich sein. Diese Anbieter können zudem die Zusammenarbeit mit vertrauenswürdigen Hinweisgebern einleiten oder verstärken und Schulungsmaßnahmen und den Austausch mit Zusammenschlüssen vertrauenswürdiger Hinweisgeber organisieren."

Artikel 22:

„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.

(3) Vertrauenswürdige Hinweisgeber veröffentlichen mindestens einmal jährlich leicht verständliche und ausführliche Berichte über die während des betreffenden Zeitraums gemäß Artikel 16 eingereichten Meldungen. In dem Bericht wird mindestens die Anzahl der Meldungen nach folgenden Kategorien aufgeführt:

a) Identität des Hostingdiensteanbieters,

b) Art der gemeldeten mutmaßlich rechtswidrigen Inhalte,

c) vom Anbieter ergriffene Maßnahmen.

Diese Berichte enthalten eine Erläuterung der Verfahren, mit denen sichergestellt wird, dass der vertrauenswürdige Hinweisgeber seine Unabhängigkeit bewahrt.

Vertrauenswürdige Hinweisgeber übermitteln dem Koordinator für digitale Dienste diese Berichte und machen sie öffentlich zugänglich. Die Informationen in diesen Berichten dürfen keine personenbezogenen Daten enthalten.

(4) Die Koordinatoren für digitale Dienste teilen der Kommission und dem Gremium die Namen, Anschriften und E-Mail-Adressen der Stellen mit, denen sie den Status des vertrauenswürdigen Hinweisgebers nach Absatz 2 zuerkannt haben bzw. deren Status als vertrauenswürdige Hinweisgeber sie im Einklang mit Absatz 6 aufgehoben oder im Einklang mit Absatz 7 aberkannt haben.

(5) Die Kommission veröffentlicht die in Absatz 4 genannten Angaben in einem leicht zugänglichen und maschinenlesbaren Format in einer öffentlich zugänglichen Datenbank und hält diese auf dem neuesten Stand. DE Amtsblatt der Europäischen Union L 277/56 27.10.2022

(6) Hat ein Anbieter von Online-Plattformen Informationen, aus denen hervorgeht, dass ein vertrauenswürdiger Hinweisgeber über die in Artikel 16 genannten Mechanismen eine erhebliche Anzahl nicht hinreichend präziser, ungenauer oder unzureichend begründeter Meldungen übermittelt hat, was auch Informationen einschließt, die im Zusammenhang mit der Bearbeitung von Beschwerden über die in Artikel 20 Absatz 4 genannten internen Beschwerdemanagementsysteme erfasst wurden, so übermittelt er dem Koordinator für digitale Dienste, der der betreffenden Stelle den Status des vertrauenswürdigen Hinweisgebers zuerkannt hat, diese Informationen zusammen mit den nötigen Erläuterungen und Nachweisen. Bei Erhalt der Information des Anbieters von Online-Plattformen und in dem Fall, dass der Koordinator für digitale Dienste der Ansicht ist, dass es berechtigte Gründe für die Einleitung einer Untersuchung gibt, wird der Status des vertrauenswürdigen Hinweisgebers für den Zeitraum der Untersuchung aufgehoben. Diese Untersuchung wird unverzüglich durchgeführt.

(7) Der Koordinator für digitale Dienste, der einer Stelle den Status des vertrauenswürdigen Hinweisgebers zuerkannt hat, widerruft diesen Status, wenn er infolge einer Untersuchung, die er auf eigene Initiative oder aufgrund von Informationen durchführt, die er von Dritten erhalten hat, auch der von einem Anbieter von Online-Plattformen nach Absatz 6 vorgelegten Informationen, feststellt, dass die betreffende Stelle die in Absatz 2 genannten Bedingungen nicht mehr erfüllt. Bevor er diesen Status widerruft, gibt der Koordinator für digitale Dienste der Stelle Gelegenheit, sich zu den Ergebnissen seiner Untersuchung und zu dem beabsichtigten Widerruf des Status der Stelle als vertrauenswürdiger Hinweisgeber zu äußern.

(8) Die Kommission gibt nach Anhörung des Gremiums, soweit erforderlich, Leitlinien heraus, um die Anbieter von Online-Plattformen und die Koordinatoren für digitale Dienste bei der Anwendung der Absätze 2, 6 und 7 zu unterstützen."

5.2 Aktuelle Liste von Typologien rechtswidriger Inhalte

Diese Liste wurde in Kontakt mit der Europäischen Kommission erstellt, um die Entwicklung harmonisierter Ansätze zur Umsetzung des DSA zu unterstützen. Die Liste erhebt keinen Anspruch auf Vollständigkeit und hat lediglich demonstrativen Charakter. Sie spiegelt potenzielle Bereiche rechtswidriger Inhalte in den Mitgliedstaaten (daher ist zu beachten, dass sie nicht in jedem Mitgliedstaat illegal sind oder sein müssen), die für die antragstellenden Einrichtungen von Interesse sein könnten, wider, darunter (keineswegs abschließend):

- Tierschutz, insbesondere
  - Tierverletzung
  - Illegaler Verkauf von Tieren und/oder Schmuggel von Wildtieren

- Verstöße gegen den Datenschutz und die Privatsphäre, insbesondere
  - Verletzung biometrischer Daten
  - Fehlender Verarbeitungsgrund für Daten
  - Verstöße gegen das Recht auf Vergessenwerden
  - Datenfälschung
  - Andere DSGVO-Datenverstöße

- Rechtswidrige Äußerungen, insbesondere
  - Verleumdung
  - Diskriminierung
  - Hassrede
  - Androhung von Gewalt (z.B. Todesdrohungen)
  - Holocaust-Leugnung

- Verstöße gegen geistiges Eigentum/andere gewerbliche Rechte, insbesondere
  - Urheberrechtsverletzungen
  - Verletzung von Geschmacksmustern
  - Verletzung von Sportrechten
  - Verletzung von Patenten
  - Verletzung von Geschäftsgeheimnissen
  - Verletzung von Markenrechten
  - Gefälschte Produkte

- Negative Auswirkungen auf die öffentliche Debatte oder auf Wahlen, insbesondere
  - Informationsmanipulation und Einmischung von außen
  - Informationsmanipulation mit dem Ziel der Beeinflussung des Ergebnisses von Wahlen

- Verpöntes Verhalten
  - Unerlaubtes Teilen von Bildern

  - Verpönte Elemente, die Deepfake- oder ähnliche Technologien enthalten
  - Doxing (öffentliche Bereitstellung persönlich identifizierbarer Informationen über eine Person)

- Online-Mobbing/Einschüchterung
  - Stalking (einschließlich aller Arten öffentlicher Hassreden, unabhängig von Medium und Inhalt wie etwa durch Bilder, Videos, Texte, öffentliche Verbreitung)
  - Sexuelle Belästigung

- Pornografie oder sexualisierte Inhalte
  - Sexueller Missbrauch durch Bilder
  - Vergewaltigung und andere sexualisierte Gewalt (Darstellung von Vergewaltigung und Aufforderung zur Vergewaltigung)

- Beeinträchtigung von Minderjährigen
  - Versäumnis, altersspezifische Beschränkungen für Minderjährige umzusetzen
  - Kinderpornografie/Material über sexuellen Missbrauch von Kindern
  - Grooming/sexuelle Verlockung von Minderjährigen

- Gefahr für die öffentliche Sicherheit
  - Provokation oder Anstiftung zur Begehung einer die öffentliche Sicherheit gefährdenden Straftat
  - Illegale Organisationen
  - Risiko für Umweltschäden
  - Gefahr für die öffentliche Gesundheit
  - Terroristische Inhalte

- Betrug und/oder Täuschung
  - Nicht authentische Konten
  - Nicht authentische Inserate
  - Nicht authentische Nutzerbewertungen
  - Identitätswechsel oder Kontokaperung
  - Phishing
  - Pyramidensysteme

- Anstiftung zur Selbstbeschädigung
  - Inhalte, die Essstörungen fördern
  - Anstiftung zur Selbstverstümmelung
  - Anstiftung zum Selbstmord

- Nicht-Beschränkung des Zugangs zur Plattform/zu den Inhalten
  - Nichtumsetzung altersspezifischer Beschränkungen
  - Nichteinhaltung von Sprachanforderungen
  - Andere diskriminierende Zugangsbeschränkungen

- Unsichere und/oder illegale Produkte

- Unzureichende Informationen über Gewerbetreibende
- Illegales Angebot von regulierten Waren und Dienstleistungen (z.B. Gesundheit)
- Verkauf von nicht-konformen Produkten (z.B. gefährliches Spielzeug)
- Illegaler Drogen- und Waffenschmuggel
- Illegale Praktiken nach dem Verbraucherschutzrecht
- Malware und Ransomware

- Gewalt
  - Koordinierter Schaden
  - Geschlechtsspezifische Gewalt
  - Menschliche Ausbeutung
  - Menschenhandel