hängt davon ab, ob er eine **wesentliche Verbindung zur Union** aufweist. Eine solche Verbindung besteht dann, wenn

- der Dienstanbieter seine Niederlassung in der Union hat, **oder**
- die Zahl der Nutzer in einem oder mehreren Mitgliedstaaten im Verhältnis zur Bevölkerung erheblich ist, **oder**
- die Tätigkeiten auf einen oder mehrere Mitgliedstaaten ausgerichtet sind (Art 3 lit e DSA).

Erheblichkeit der Nutzerzahl

Ab wann die Zahl der Nutzer in einem Mitgliedstaat im Verhältnis zu Bevölkerung „erheblich" ist, lässt der europäische Gesetzgeber leider offen. In **analoger Anwendung** könnten die Überlegungen zu sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen herangezogen werden: Nach diesen liegt eine **„erhebliche Reichweite"** dann vor, wenn die Nutzerzahl eine operative Schwelle von 45 Millionen, das bedeutet 10 % der Bevölkerung der Union, erreicht (ErwGr 76 DSA). Allerdings muss man feststellen, dass diese Schwelle sich auf die Qualifikation als „sehr große" Plattform/Suchmaschine bezieht. Der Begriff der „erheblichen Anzahl" an Nutzern wird in Zusammenhang mit Gefahren, die von diesen sehr großen Anbietern ausgehen, im DSA verwendet (ErwGr 137 DSA). Um den Anwendungsbereich des DSA nicht übermäßig zu schmälern, muss mE deshalb davon ausgegangen werden, dass die Schwelle für eine erhebliche Anzahl von Nutzern wohl **jedenfalls unter 10 %** der Bevölkerung eines Mitgliedstaates liegt.

Anleihe kann ggf auch bei der **DSGVO** genommen werden: Nach Art 37 DSGVO ist unter anderem dann ein Datenschutzbeauftragter zu bestellen, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der **„umfangreichen Verarbeitung"** bestimmter Datenkategorien besteht. Auch hier lässt der Gesetzgeber zwar konkrete Schwellenwerte vermissen, gibt dem Anwender in der Praxis jedoch zumindest bestimmte, wenn auch generische, Kriterien an die Hand. Aus den Erwägungsgründen ergibt sich, dass dieses Kriterium dann erfüllt sein kann, wenn *„große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene"* verarbeitet werden und *„eine große Zahl von Personen"* betroffen ist (ErwGr 91 DSGVO). Ein früher Entwurf der DSGVO sah vor, dass eine Verarbeitung dann umfangreich ist, wenn eine Anzahl von 5.000 Personen innerhalb von 12 Monaten betroffen ist.[49] Diese konkrete Schwelle wurde allerdings nicht beibehalten, weshalb sie nicht zur Beurteilung der Erheblichkeitsschwelle herangezogen werden kann. Auch liegt diese Empfehlung bereits so weit zurück, dass sie die aktuellen Gegebenheiten von Online-Prozessen nicht mehr abbildet.

49 COM (2012)0011 – C7-0025/2012 – 2012/0011 (COD).

bestimmt. Durch das im ECG festgelegte und nunmehr im DSA präzisierte Haftungsregime werden keine neuen Haftungsvoraussetzungen für Diensteanbieter geschaffen.[87]

Prägnant: Art 4 ff stellen Regeln zur Haftungsbegrenzung auf, nicht zur Haftungsbegründung![88]

Ebenso zu beachten ist, dass es sich bei der Haftungsbefreiung lediglich um eine **deliktische Privilegierung**, nicht aber um eine Freistellung von vertraglichen Sachverhalten handelt. Der Ausschluss der Verantwortung betrifft zwar sowohl das **Strafrecht** als auch das **Zivilrecht** und das **öffentliche Recht**, allerdings nur hinsichtlich der deliktischen Haftung. Das bedeutet, dass sich „Access-Provider" (oder nunmehr Diensteanbieter der reinen Durchleitung) bspw hinsichtlich Downtime-Szenarien, in denen ihr Dienst gar nicht oder bloß eingeschränkt verfügbar ist und diese Downtime einen **Verstoß gegen vertragliche Bestimmungen** darstellt, **nicht** auf die **Haftungsprivilegierungen** des Art 4 DSA berufen können.[89]

3.3. Haftung von Anbietern einer reinen Durchleitung (Art 4)

Art 4 regelt die Haftungsfreistellung für Anbieter von reinen Durchleitungsdiensten. Diese Anbieter **übermitteln Informationen** in einem Kommunikationsnetz oder **vermitteln den Zugang** zu einem **Kommunikationsnetz** (siehe dazu im Detail Kapitel 2.3.2.1.).

Die Haftungsfreistellung gilt unter folgenden Bedingungen:

- Informationen stammen vom Nutzer: Es handelt sich um von einem Nutzer bereitgestellte Informationen.
- Keine Veranlassung der Übermittlung: Der Anbieter darf die Übermittlung der Informationen nicht veranlassen.
- Keine Auswahl des Adressaten: Der Anbieter darf den Adressaten der übermittelten Informationen nicht auswählen.
- Keine Auswahl oder Veränderung der Informationen: Der Anbieter darf die übermittelten Informationen weder auswählen noch verändern.

3.3.1. Tatbestandsmerkmale

Die oben genannten Vorgaben stellen sicher, dass der Anbieter eine rein **passive Rolle** einnimmt und somit nicht für die übermittelten Informationen haftbar gemacht werden kann. Die Tätigkeit des Anbieters einer „reinen Durchleitung" erschöpft sich grundsätzlich in der **neutralen** und (üblicherweise) **automatisierten** laufenden **Weiterleitung** der vom Nutzer eingegebenen Informationen. Eine aktive Veranlassung der Übermittlung oder eine Kontrolle der übermittelten Informationen findet dabei nicht statt. Aus diesem Grund wird hier, im Unterschied zu den folgenden Haftungsbestimmungen der übrigen Diensteanbieter iSd

87 *Ciresa* in *Schwimann/Kodek* (Hrsg), ABGB Praxiskommentar[5] (2021) zu § 13 ECG Rz 1; RIS-Justiz RS0118525.

88 *F. Hofmann* in *Hofmann/Raue*, NK-DSA Vor Art 4 C. I.

89 Vgl zum Vorgänger des § 13 ECG bereits *Zankl*, E-Commerce-Gesetz[2] (2015) Rz 217 mwN.

lich.[163] Aber auch Anordnungen zur Bereitstellung von aggregierten Informationen, die für statistische Zwecke oder eine faktenbasierte Politikgestaltung erforderlich sind, sind von dieser Ausnahme betroffen.[164] Daher kommen in diesen Fällen nicht die in der Folge dargelegten Regeln des DSA zur Anwendung.

4.2. Mindestanforderungen an Anordnungen

Mit dem DSA wurde ein „Mindestqualitätsstandard" für behördliche Anordnungen zum Vorgehen gegen rechtswidrige Inhalte und Auskunftsanordnungen geschaffen. Diese Mindestanforderungen umfassen **Formvorschriften**, wie den Mindestinhalt (Kapitel 4.2.1.), die Sprache, in der die Anordnung zu übermitteln ist, (Kapitel 4.2.4.) sowie die Übermittlungsform der Anordnungen (Kapitel 4.3.). Zusätzlich wurden aber **auch materiellrechtliche Grenzen** festgelegt, die den Wirkungsumfang dieser behördlichen Anordnungen beschränken: Bei Anordnungen zum Vorgehen gegen rechtswidrige Inhalte betrifft dies deren räumlichen Geltungsbereich (Kapitel 4.2.2.) und bei Auskunftsanordnungen die beim Provider verfügbaren Informationen (Kapitel 4.2.3.).

Aus der Formulierung der Bestimmungen ergibt sich, dass diese Mindestanforderungen erst im Zeitpunkt der Übermittlung an den Provider erfüllt sein müssen.[165] Davor, also insbesondere beim Erlass der Anordnung, müssen sie noch nicht zwingend vorliegen. Daher bleibt es den Behörden zum Beispiel möglich, die Anordnungen vorerst in der Amtssprache zu erlassen und später erst übersetzt an den Provider zu übermitteln (siehe im Detail Kapitel 4.2.4.).

4.2.1. Mindestinhalt

Anordnungen zum Vorgehen gegen rechtswidrige Inhalte sowie Auskunftsanordnungen haben den folgenden **allgemeinen Mindestinhalt** aufzuweisen:

- **Angaben zur Rechtsgrundlage**
  Der DSA schafft keine eigene Rechtsgrundlage für Anordnungen. Vielmehr ergibt sich diese auf Grundlage des geltenden Unionsrechts oder des nationalen Rechts im Einklang mit dem Unionsrecht. Je nach handelnder Behörde kommen daher unterschiedliche Rechtsgrundlagen in Betracht. Um Missverständnisse zu vermeiden, sollte daher jedenfalls auf die einschlägige Rechtsnorm oder Rechtsprechung, aus der sich die Rechtsgrundlage ergibt, verwiesen werden, zB bei Verletzung von Urheberrechten durch Verweis auf §§ 81 f UrhG (Unterlassungs- und Beseitigungsanspruch) oder bei der Auskunft über Stammdaten zur Aufklärung eines konkreten Verdachts einer Straftat durch Verweis auf § 135 Abs 1a StPO.

163 § 134 Z 1b StPO iVm § 135 Abs 1a StPO.
164 ErwGr 37 DSA.
165 Art 9 Abs 2; Art 10 Abs 2 DSA.

Wesentliche Branchen, die vom NISG erfasst sind (exemplarisch)

Diese Schlüsselbranchen sind

- Energie,
- Verkehr,
- Bankwesen,
- Finanzmarktinfrastrukturen,
- Gesundheitswesen,
- Trinkwasserversorgung und
- digitale Infrastruktur.

Welche wesentlichen Dienste innerhalb dieser Schlüsselbranchen konkret dem NISG unterliegen, wird in der NISV **konkretisiert**. So sind im Sektor „Energie", Teilsektor „Elektrizität" im Bereich der Stromverteilung etwa Verteilernetzbetreiber erfasst, wenn über deren Verteilernetz Elektrizität an mehr als 88.000 Zählpunkte transportiert wird, oder wenn dieses in einer Landeshauptstadt gelegen ist.[198]

Anbieter digitaler Dienste sind juristische Personen oder eingetragene Personengesellschaften, die einen **digitalen Dienst** in Österreich anbieten und eine **Hauptniederlassung in Österreich** haben oder einen **Vertreter** in Österreich namhaft gemacht haben. **Explizit ausgenommen** sind natürliche Personen, Kleinstunternehmen und kleine Unternehmen (Unternehmen mit weniger als 50 Mitarbeitern und einem Jahresumsatz bzw einer Jahresbilanz von unter EUR 10 Mio). Die Größenschwellen ergeben sich anhand der einschlägigen **Empfehlung der EU-Kommission**.[199]

Digitale Dienste iSd NISG sind **Online-Marktplätze**, **Online-Suchmaschinen** oder **Cloud-Computing-Dienste**. Diese Dienste müssen grundsätzlich entgeltlich, im Fernabsatz, elektronisch sowie auf individuellen Abruf erbracht werden. Diese Subsumtion orientiert sich an der Definition der RL (EU) 2015/1535[200] (siehe dazu auch Kapitel 2.3.1.).

5.1.1.3. Sicherheitsvorkehrungen

Anbieter digitaler Dienste haben in Hinblick auf die Netz- und Informationssysteme, die sie **für die Bereitstellung des digitalen Dienstes** nutzen, **geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen** zu treffen. Diese haben unter Berücksichtigung des **Stands der Technik** ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, das dem bestehenden, mit vernünftigem Aufwand **feststellbaren Risiko angemessen** ist. Bei den Sicherheitsvorkehrungen müssen berücksichtigt werden:

- die Sicherheit der Systeme und Anlagen;
- die Bewältigung von Sicherheitsvorfällen;

198 Vgl § 4 Abs 1 Z 1 lit b NISV.

199 Empfehlung der Kommission vom 6.5.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, ABl. L 124 vom 20.5.2003.

200 Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft.

Um sicherzustellen, dass die Cybersicherheitsbehörde ihre Aufsichtstätigkeit wirksam ausüben kann, haben Anbieter digitaler Dienste der Cybersicherheitsbehörde **geplante Prüfungen spätestens einen Monat vor deren Beginn** mitzuteilen und dabei auch **einen Prüfplan zu übermitteln**, aus dem hervorgeht, zu welchem Zeitpunkt oder zu welchen Zeitpunkten die unabhängige Stelle durch welche unabhängigen Prüfer und an welchen Standorten des jeweiligen Anbieters digitaler Dienste prüfen wird.

Außerdem ist die Cybersicherheitsbehörde befugt, die Prüfer von unabhängigen Stellen bei ihren Prüfhandlungen im Rahmen von Prüfungen bei Anbietern digitaler Dienste kontrollierend zu begleiten (**„Witnessaudits"**).

5.1.3.4.3. Durchsetzungsmaßnahmen

Stellt die Cybersicherheitsbehörde im Rahmen ihrer Aufsichtstätigkeit fest, dass ein Anbieter digitaler Dienste seinen Verpflichtungen nach dem NISG 2024 **nicht nachkommt**, so hat sie diesen in einem **ersten Schritt** insbesondere darauf hinzuweisen, bestimmte spezifische Umsetzungsmaßnahmen oder Adaptierungen im Bereich konkreter Risikomanagementmaßnahmen und hinsichtlich der Einhaltung von Berichtspflichten oder sonstigen Verpflichtungen vorzunehmen. Dies ist zunächst als **bloße Information** der Cybersicherheitsbehörde an den jeweiligen Anbieter digitaler Dienste zu verstehen. Gegebenenfalls können dabei auch **angemessene Fristen in Form einer Verfahrensanordnung** gesetzt werden.

Wird einer solchen Verfahrensanordnung **nicht nachgekommen**, hat dies zur Folge, dass die jeweils angeordnete Maßnahme, wie etwa die (vollständige) Umsetzung jeweiliger Risikomanagementmaßnahmen, durch die Cybersicherheitsbehörde in einem **weiteren Schritt mit Bescheid** angeordnet wird.

Neben der Anordnung von Risikomanagementmaßnahmen ist die Cybersicherheitsbehörde befugt, den Anbieter digitaler Dienste aufzufordern, die **Nutzer seiner Dienste und Tätigkeiten** (etwa Kunden) über eine Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen **zu informieren** oder die **Öffentlichkeit** über **Aspekte seiner Verletzung des NISG 2024** zu informieren.

5.1.3.4.4. Strafen

Die Strafrahmen der NIS-2-RL wurden in das NISG 2024 **wörtlich übernommen**.

Für Verstöße gegen die Verpflichtungen des NISG 2024 sind Verwaltungsstrafen von den Bezirksverwaltungsbehörden als zuständige Behörden nach den verfahrensrechtlichen Bestimmungen des VStG 1991[232] zu verhängen.

Diese „Verwaltungsübertretungen" betreffen zB Verstöße von Anbietern digitaler Dienste gegen die Verpflichtung zur Durchführung von Cybersicherheitsschu-

232 Verwaltungsstrafgesetz 1991 – VStG, BGBl 52/1991.

werden bei **verhaltensorientierter Werbung** Anzeigen basierend auf dem bisherigen Surfverhalten eines Nutzers angezeigt. Hat der Nutzer etwa kürzlich nach Jacken gesucht, wird, während er sich auf ganz anderen Webseiten, etwa Reisebuchungsportalen, aufhält, Werbung für Jacken von verschiedenen Marken angezeigt.

Praxistipp

Werbung sollte durch **visuelle oder akustische Kennzeichnung** deutlich hervorgehoben werden, um sie von anderen Inhalten klar zu unterscheiden.

Anbieter von Online-Plattformen sind gemäß Art 26 Abs 2 DSA zudem verpflichtet, den Nutzern eine **Funktion** zur Verfügung zu stellen, mit der sie erklären können, ob der von ihnen bereitgestellte Inhalt Werbung darstellt oder eine solche enthält.

Praxistipp

Diese Funktion kann anhand folgender Praktiken zur Verfügung gestellt werden:

- **Checkbox bei der Inhaltserstellung:** Ein Kästchen, das Nutzer beim Hochladen von Inhalten ankreuzen können, um anzugeben, ob Werbung enthalten ist.
- **Dropdown-Menü:** Eine Auswahloption, bei der Nutzer den Inhalt als „Werbung", „gesponsert" oder „keine Werbung" kennzeichnen können.
- **Tagging-System:** Ein System, bei dem Nutzer ihre Inhalte mit Tags wie „Werbung" oder „sponsored" versehen können.
- **Textfeld für Offenlegung:** Ein Feld, in dem Nutzer erklären können, ob ihr Inhalt kommerzielle Kommunikation enthält.

Wird eine solche Erklärung abgegeben, müssen Anbieter von Online-Plattformen sicherstellen, dass die anderen Nutzer klar, eindeutig und in Echtzeit erkennen können, dass der Inhalt Werbung darstellt oder enthält.

Anbieter von Online-Plattformen dürfen gemäß Art 26 Abs 3 DSA keine Werbung anzeigen, die auf **Profiling** iSd Art 4 Z 4 DSGVO **unter Verwendung besonderer Kategorien personenbezogener Daten** beruht. Dies umfasst Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Achtung!

Unter der DSGVO kann es erlaubt sein, besondere Kategorien personenbezogener Daten, die auf Profiling beruhen, für Werbezwecke zu verarbeiten. Dies kommt dann in Frage, wenn ein Rechtfertigungstatbestand iSd Art 9 DSGVO vorliegt, insb wenn eine Einwilligung erteilt wird. Nach dem DSA sind diese Werbepraktiken aber jedenfalls verboten.

Da die Informationspflicht nach dem DSA auch aussagekräftige Informationen über die wichtigsten Parameter zur Bestimmung der Zielgruppe umfassen, geht sie auch dann über jene der DSGVO hinaus, wenn keine besonderen Kategorien personenbezo-

- **Eindeutige Angabe des Speicherorts**
  - zB URL oder URI
  - Möglichkeit weiterer zweckdienlicher Hinweise
  - Möglichkeit der Angabe mehrerer Links zu verschiedenen mutmaßlich rechtswidrigen Inhalten
- **Begründete Erläuterung**
  - ohne unverhältnismäßige Zeichenbeschränkung
- **Gutglaubenserklärung**
  - zur Missbrauchsvermeidung von Falschmeldungen

Optionaler, aber empfehlenswerter Inhalt:

- **Kategorie des rechtswidrigen Inhalts**
  - inkl Kategorie für nicht aufgezählte Kategorien, etwa „Sonstige rechtswidrige Inhalte"
- **Möglichkeit, Anhänge hochzuladen**

6.1.3. Empfangsbestätigung

Sobald eine Meldung eingeht, die eine elektronische Kontaktangabe der meldenden Person enthält (zB eine E-Mail-Adresse), muss der Hosting-Provider unverzüglich den Empfang der Meldung bestätigen. Hier empfehlen sich automatische Empfangsbestätigungen, etwa via E-Mail.

6.1.4. Tatsächliche Kenntnis und Bewusstsein

Eine ordnungsgemäße Artikel-16-Meldung bewirkt, dass damit von einer tatsächlichen Kenntnis bzw einem Bewusstsein des Hosting-Providers in Bezug auf die Rechtswidrigkeit des gemeldeten Inhalts ausgegangen wird. Das erfordert, dass es aufgrund der Angaben in der Meldung einem sorgfältig handelnden Hosting-Provider möglich ist, ohne eingehende rechtliche Prüfung festzustellen, dass der einschlägige Inhalt rechtswidrig ist. Es handelt sich dabei um eine **unwiderlegbare Vermutung der Kenntnis**.[293] Der Provider kann sich daher nicht freibeweisen, indem er nachweist, dass er trotz Meldung gar keine Kenntnis hatte. Handelt der Hosting-Provider dann nicht zügig und setzt Maßnahmen, um gegen den rechtswidrigen Inhalt vorzugehen, verliert der Hosting-Provider sein Haftungsprivileg und wird haftbar.

Damit der Hosting-Provider ohne eingehende rechtliche Prüfung die Rechtswidrigkeit des gemeldeten Inhalts überprüfen kann, sollte die Meldung daher zumindest

- eine eindeutige Angabe zum Speicherort des/der vermutlich rechtswidrigen Inhalts/Inhalte,
- eine hinreichend begründete Erläuterung zum jeweils gemeldeten Inhalt und
- – soweit erforderlich – Angaben zur Identifikation der meldenden Person enthalten (siehe 6.1.2.).

293 *Raue* in *Raue/Hofmann*, NK-DSA (2023) Art 16 Rz 55.

Konzepte verständlich zu machen, sollten konkrete Beispiele und klare Erklärungen verwendet werden. Dabei hilft es auch, wichtige Informationen hervorzuheben, etwa durch Fettschrift, und die Begründung in übersichtliche Absätze oder Bulletpoints zu gliedern. Die Begründung hat in der Sprache zu erfolgen in der der Hosting-Dienst auch vom betroffenen Nutzer verwendet wird. Sollte der Hosting-Provider daher automatische Tools bei der Erstellung der Begründung, insbesondere Übersetzungstools, verwenden, sollte darauf geachtet werden, dass diese Tools auch die geforderte Qualität bieten.

Darüber hinaus muss die Begründung so **genau und spezifisch wie möglich** sein. Allgemeine Textbausteine und unkonkrete Formulierungen sind zu vermeiden. Der Hosting-Provider muss sich in der Begründung mit dem konkreten, beanstandeten Inhalt auseinandersetzen und erläutern, warum die genannte Rechtsgrundlage gerade in diesem Fall zutrifft. Es ist daher von unkonkreten Floskeln wie *„der Inhalt verstößt gegen die AGB"* oder *„der Inhalt ist rechtswidrig"* abzusehen.[316] Stattdessen sollte die Begründung so formuliert sein, dass der betroffene Nutzer genau verstehen kann, warum die Maßnahme getroffen wurde, sodass er in der Lage ist, auf die Entscheidung mit den verfügbaren Rechtsbehelfen zu reagieren. Der betroffene Nutzer soll nicht mit Fragezeichen zurückgelassen werden und keine Ahnung haben, was er falsch gemacht hat. Daher ist eine präzise und nachvollziehbare Darstellung der Gründe und Umstände der Entscheidung gefordert.

Schließlich hat der Hosting-Provider die Begründung dem betroffenen Nutzer **elektronisch zu übermitteln**. Darüber hinaus haben bestimmte Plattform-Provider die Begründung an die Europäische Kommission in maschinenlesbarer Form zu übermitteln, sodass diese in der DSA-Transparenz-Datenbank veröffentlicht werden kann (siehe dazu 5.2.1.4.).

Muster: Begründung des Hosting-Provider bei beschränkender Maßnahme

Begründung bei urheberrechtlich geschütztem Inhalt

Wir haben eine Meldung zu folgendem Inhalt erhalten:

[Eingebetteter Link bzw Screenshot zum Inhalt]

Nach Prüfung der Meldung haben wir den gemeldeten Inhalt auf unbestimmte Zeit in Österreich **gesperrt**.

Begründung: Die Meldung erfolgte durch den Rechteinhaber *[Name des Rechteinhabers]* **des urheberrechtlich geschützten Werks** *[Titel des Werks]*. Der Meldung zufolge haben Sie das geschützte Werk ohne Zu-

316 Vgl *Raue* in *Raue/Hofmann*, NK-DSA (2023) Art 17 Rz 57.

und kann von einer reinen Initialzündung über die organisatorische Einbettung und Betreuung bis hin zu finanziellen Förderungsmaßnahmen reichen.[403] Die politische und rechtliche Relevanz konkreter Themenfelder sowie die Intensität der potenziellen Auswirkungen dürften dabei entscheidende Faktoren für die Art der Verfahrenswahl und den Grad der Involviertheit von EU-Kommission und Gremium sein.

Aufgrund der enormen Bedeutung und den erheblichen Auswirkungen von Hate Speech und Desinformationen war daher bspw bei der Erarbeitung entsprechender Verhaltenskodizes (jedoch vor Inkrafttreten des DSA) eine sehr engmaschige und intensive Steuerung durch die EU-Kommission zu beobachten.

Einen Sonderfall enthält Art 45 Abs 2 DSA. Bei Vorliegen der dort genannten Voraussetzungen (insbesondere das Auftreten systemischer Risiken iSd Art 34 Abs 1 DSA) kann die EU-Kommission die betroffenen Anbieter (zB VLOPs und VLOSEs, aber auch andere Unternehmen und Organisationen der Zivilgesellschaft) explizit dazu auffordern, sich an der Erarbeitung von Verhaltenskodizes zu beteiligen. Das Auftreten systemischer Risiken führt damit zu einer Schärfung des behördlichen Handlungsauftrages, der sich von einem bloßen Förderungsauftrag in eine Aufforderungskompetenz umwandelt. Zu den rechtlichen Implikationen einer solchen Aufforderung durch die EU-Kommission und der Verweigerung einer Mitwirkung siehe näher unter 8.2.

8.1.3.3. Inhaltliche Mindestvorgaben, Überwachungs- und Transparenzvorgaben

Wie beschrieben ist die Erarbeitung von Verhaltenskodizes sowie die Beteiligung an ihnen grundsätzlich freiwillig ausgestaltet (mit Ausnahme von Art 45 Abs 2 DSA). Damit korrespondierend gewährt der DSA den betroffenen Unternehmen und Akteuren erhebliche Freiräume. Da die Verhaltenskodizes jedoch ersichtlich darauf abzielen, zur ordnungsgemäßen Anwendung des DSA und der Erfassung und Minimierung von etwaigen Risiken beizutragen, wird der Spielraum durch inhaltliche Mindestvorgaben sowie Überwachungs- und Transparenzvorgaben eingezäunt. Hierdurch wird sichergestellt, dass sich die Selbstregulierung im Rahmen und in den Grenzen eines gesetzlichen Korsetts entfaltet.

Mit Blick auf die inhaltlichen Mindestvorgaben ist Art 45 DSA zurückhaltend formuliert. Zum einen muss nach Art 45 Abs 3 DSA das mit Verhaltenskodizes spezifisch verfolgte Ziel klar dargelegt werden. Damit verbunden sollen die EU-Kommission und das Gremium sich hinsichtlich des Inhaltes der Kodizes dafür einsetzen, dass dieser auch den Bedürfnissen und Interessen aller Beteiligten (insbesondere den Bürgern auf Unionsebene) Rechnung trägt. Weiterhin müssen in Verhaltenskodizes wesentliche Leistungsindikatoren festgelegt werden, anhand

403 Vgl näher dazu *Wagner* in *Müller-Terpitz/Köhler*, DSA-Kommentar (2024) Art 45 DSA Rn 10.

Verpflichtung zur Duldung von Nachprüfungen und Widerstand

Anbieter von VLOPs/VLOSEs sowie andere betroffene Personen müssen Nachprüfungen **dulden**, wenn diese von der EU-Kommission durch einen **förmlichen Beschluss** angeordnet wurden. Dieser Beschluss muss (i) den Gegenstand und Zweck der Nachprüfung definieren, (ii) das Datum des Beginns der Nachprüfung festlegen, (iii) die Sanktionen gemäß den Art 74 und 76 DSA anführen, und (iv) auf Rechtsschutzmöglichkeiten hinweisen. Die Duldungspflicht des Anbieters kann mit Zwangsgeldern (Art 76 Abs 1 lit b DSA) durchgesetzt werden. Vor dem Erlass des Beschlusses konsultiert die Kommission den Koordinator des betroffenen Mitgliedstaates (Abs 6).

Sollte sich der Anbieter bzw die betroffene Person einer Nachprüfung **widersetzen**, kann die EU-Kommission den Mitgliedstaat, in dessen Hoheitsgebiet die Nachprüfung durchgeführt wird, um die erforderliche Unterstützung ersuchen. Diese Unterstützung kann, falls erforderlich und nach nationalem Recht zulässig, auch Zwangsmaßnahmen durch die zuständigen Strafverfolgungsbehörden umfassen, damit die Nachprüfung durchgeführt werden kann (Abs 8).

9.4.3.4. Verpflichtungszusagen (Art 71 DSA)

Im Rahmen von Verfahren nach dem DSA hat die EU-Kommission die Befugnis, Verpflichtungszusagen von Anbietern von VLOPs/VLOSEs zu akzeptieren. Das Instrument der Verpflichtungszusage ist auch in anderen Bereichen des Unionsrechts (zB Wettbewerbsrecht) gebräuchlich und soll im Rahmen des DSA dazu dienen, die Einhaltung der einschlägigen Bestimmungen sicherzustellen. Verpflichtungszusagen können Maßnahmen oder Verhaltensänderungen umfassen, die der Anbieter freiwillig anbietet, um potenzielle oder festgestellte Verstöße zu beheben. Das kann sowohl für die EU-Kommission als auch für den betreffenden Anbieter attraktiv sein: Auf Seiten der EU-Kommission kann dies zu erheblichen Zeit- und Ressourceneinsparungen führen, wodurch eine effizientere Verfahrensführung ermöglicht wird. Für den Anbieter bietet diese Möglichkeit den Vorteil, der möglichen öffentlichen Stigmatisierung durch einen Beschluss über die Nichteinhaltung des DSA sowie der Verhängung einer Geldbuße zu entgehen.[490]

Kommt die EU-Kommission zu dem Ergebnis, dass die angebotenen Verpflichtungszusagen **ausreichend** sind, um die Einhaltung der Verordnung zu gewährleisten, so kann sie diese mit **Beschluss für bindend erklären** und feststellen, dass sie nicht weiter tätig wird (Abs 1). Sollte die Kommission bei Prüfung der Verpflichtungszusagen hingegen zu der Auffassung gelangen, dass diese nicht ausreichen, dann lehnt sie die angebotenen Verpflichtungszusagen im Wege eines begründeten Beschlusses ab (Abs 3). Das Verfahren wird daraufhin ohne verbindliche Zusagen abgeschlossen und die Kommission kann gegebenenfalls Durchsetzungsmaßnahmen ergreifen.

490 *Bartels* in *Kraul* (Hrsg), Das neue Recht der Digitalen Dienste (2023) § 5 Rz 40.