

In Kooperation mit: **Bitkom** – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · **davit im DAV** – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · **eco** – Verband der Internetwirtschaft e.V. · **game** – Verband der deutschen Games-Branche e.V. · **Legal Tech Verband** Deutschland e.V. · **VAUNET** – Verband Privater Medien

Beilage zu MMMR 8/2025

HERAUSGEBER

RAin **Dr. Astrid Auer-Reinsdorff**, FA IT-Recht, Berlin/Lissabon – **Prof. Dr. Maximilian Becker**, Lehrstuhl für Bürgerliches Recht, Immaterialgüterrecht und Medienrecht, Universität Siegen – **Paula Cypierre**, Director of Data Ethics & Innovation, ada Learnings GmbH, Düsseldorf – RA **Dr. habil. Christian Förster**, Partner, Bartsch Rechtsanwälte, Karlsruhe – **Prof. Dr. Nikolaus Forgó**, Professor für Technologie- und Immaterialgüterrecht und Vorstand des Instituts für Innovation und Digitalisierung im Recht, Universität Wien – RAin **Prof. Dr. Sibylle Gierschmann**, LL.M. (Duke University), FA Urheber- und Medienrecht, Hamburg – RA **Prof. Dr. Christian-Henner Hentsch**, M.A., LL.M., Leiter Recht und Regulierung beim game – Verband der deutschen Games-Branche e.V., Berlin/Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln – **Prof. Dr. Thomas Hoeren**, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. em. Dr. Bernd Holznapel**, ehem. Direktor der Öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Lena Hornkohl**, LL.M., Tenure Track Professor für Europarecht, Universität Wien/Institut für Europarecht, Internationales Recht und Rechtsvergleichung – RAin **Dr. Andrea Huber**, LL.M. (USA), Berlin – **Prof. Dr. Katharina Kaesling**, LL.M., Juniorprofessor für Bürgerliches Recht, Geistiges Eigentum, insbesondere Patentrecht, sowie Rechtsfragen der KI, TU Dresden – **Prof. Dr. Dennis-Kenji Kipker**, Legal Advisor, Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) e.V., Kompetenzzentrum Informationssicherheit + CERT@VDE/Research Director Cyberintelligence.institute, Frankfurt/M. – **Wolfgang Kopf**, LL.M., Leiter Zentralbereich Politik und Regulierung, Deutsche Telekom AG, Bonn – **Prof. Dr. Oliver Kreuzt**, LL.M., Professor für Zivilrecht mit der Vertiefungsrichtung Immaterialgüterrecht, Rechtsfragen der Digitalisierung und Wettbewerbsrecht, Ostfalia – Hochschule für angewandte Wissenschaften – **Prof. Dr. Marc Liesching**, Professor für Medienrecht und Medientheorie, HTWK Leipzig/München – **Prof. Dr. Tobias Lutz**, LL.M., MJur, Juniorprofessor für Privatrecht, Universität Augsburg – **Prof. Dr. Juliane K. Mendelsohn**, Juniorprofessorin Fachgebiet Law and Economics of Digitalization, TU Ilmenau – **Prof. Dr. Alexander Roßnagel**, Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Wiesbaden/Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel – **Prof. Dr. Christian Rüpckert**, Lehrstuhl für Strafrecht, Strafprozessrecht und IT-Strafrecht, Universität Bayreuth – RA **Dr. Raimund Schütz**, Loschelder Rechtsanwälte, Köln – **Prof. Dr. Louisa Specht-Riemschneider**, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn – RA **Dr. Axel Spies**, Morgan, Lewis & Bockius LLP, Washington DC – **Prof. Dr. Björn Steinrötter**, Lehrstuhl für Bürgerliches Recht, IT-Recht und Medienrecht, Universität Potsdam

BEIRAT DER KOOPERATIONSPARTNER

Karsten U. Bartels, LL.M., Vorsitzender der Arbeitsgemeinschaft IT-Recht (davit) im Deutschen Anwaltverein e.V. – **Daniela Beaujean**, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Medien (VAUNET), Berlin – RAin **Susanne Dehmel**, Mitglied der Geschäftsleitung Bitkom e.V., Berlin – **Stefan Schicker**, Vorstandsvorsitzender des Legal Tech Verband Deutschland e.V., Berlin

REDAKTION

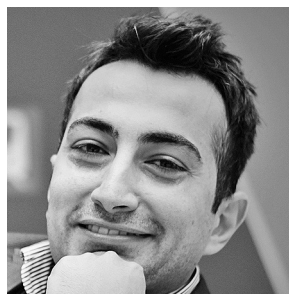
Anke Zimmer-Helfrich, Chefredakteurin – **Nina Himmelstoß**, Redakteurin – **Ruth Schrödl**, Redakteurin – **Christine Völker-Albert**, Redakteurin – **Eva Wanderer**, Redaktionsassistentin – Wilhelmstr. 9, 80801 München

EDITORIAL Aufgaben des Digital Services Coordinators

In unserem alltäglichen Leben sind wir umgeben von Vermittlungsdiensten, das sind Dienste, die Informationen übermitteln, ggf. speichern und diese für Dritte sichtbar veröffentlichen. Dies umfasst im Wesentlichen Online-Plattformen und Hosting-Dienste, aber auch Caching-Dienste und sog. Dienste der reinen Durchleitung. Die Bekanntesten nutzen wir praktisch ununterbrochen, seien es die Plattformen der sozialen Medien wie Instagram, TikTok oder X, oder Online-Marktplätze wie Amazon, Temu oder eBay.

Entsprechend groß kann der Einfluss der genutzten Vermittlungsdienste auf unsere Meinungsbildung, die eigenen Entscheidungen und unsere Sicherheit sein. Die EU-Kommission hat daher im Rahmen ihrer Digitalstrategie verschiedene Verordnungen verabschiedet, um den Einfluss der auf uns wirkenden Vermittlungsdienste regulieren zu können.

Eine dieser Verordnungen ist der DSA, dessen Ziel es ist, ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld für die Nutzenden zu schaffen. Spätestens seit dem vollständigen Inkrafttreten am 17.2.2024 sollen insbesondere die Rechte und Handlungsoptionen der Nutzenden gestärkt werden, selbst gegen rechtswidrige Inhalte, darunter auch illegale Produkte, im Internet vorgehen zu können.



Dr. Deniz Erdem

Mit Inkrafttreten des nationalen Durchführungsgesetzes zu dieser EU-Verordnung, dem Digitale-Dienste-Gesetz (DDG), am 14.5.2024 wurde die Bundesnetzagentur (BNetzA) als nationale Koordinierungsstelle für Digitale Dienste, international als Digital Services Coordinator (DSC) bezeichnet, ernannt. Seitdem nimmt sie ihre Rolle als Aufsicht von Vermittlungsdiensten sowie der Umsetzung des DSA für Deutschland wahr.

Der DSC eines jeden EU-Mitgliedstaats koordiniert dabei die Vorgänge und Informationen zwischen relevanten Marktakteuren, darunter die Vermittlungsdienste selbst, Behörden, Verbände, Unternehmen, Organisationen der Zivilgesellschaft sowie den Nutzenden.

Die Aufsichtszuständigkeit für die einzelnen Vermittlungsdienste ergibt sich dabei zunächst aus dem Sitz der EU-Hauptniederlassung der Diensteanbieter bzw. des Sitzes ihrer gemeldeten gesetzlichen Vertretung in der EU. Bei sehr großen Online-Plattformen bzw. Online-Suchmaschinen, sog. VLOPs bzw. VLOSEs (Very Large Online Platforms bzw. Very Large Online Search Engines) nimmt die EU-Kommission selbst auch die Aufgabe der Aufsicht wahr.

Um die Nutzerinnen und Nutzer bei ihren Handlungsmöglichkeiten gegen illegale Inhalte und Produkte im Internet unterstützen zu können, schafft der DSA verschiedene Instrumente. Für die Einrichtung oder die Prüfung der Einhaltung dieser Instrumente sind die nationalen DSCs verantwortlich.

Darunter fallen auch die Durchführung verschiedener Zertifizierungs- oder Zulassungsverfahren wie die Zertifizierung bzw. Zulassung von außergerichtlichen Streitbeilegungsstellen, sog. vertrauenswürdigen Hinweisgebern (auch bezeichnet als Trusted Flagger) sowie Forschenden sofern diese bei VLOPs und VLOSEs einen Antrag auf dort vorhandene Daten vorbringen.

Außergerichtliche Streitbeilegungsstellen vermitteln nach Ihrer Zertifizierung im Wesentlichen zwischen den Nutzenden und Online-Plattformen, sofern Nutzende mit der Entscheidung einer Online-Plattform hinsichtlich der Entfernung eines Inhalts oder der Sperrung oder Löschung eines Kontos nicht einverstanden sind. Nach ihrer Zulassung melden Trusted Flagger vermutete rechtswidrige Inhalte an Online-Plattformen, die diese Meldungen daraufhin bevorzugt bearbeiten und prüfen müssen. Zugelassene Forschende erhalten einen angefragten und bestätigten Datenzugang zu Daten von Online-Plattformen, die die Forschenden in ihren Untersuchungen zu sog. systemischen Risiken und deren Minderung benötigen.

Der DSA schafft darüber hinaus weitere Instrumente für die Nutzenden, um gegen rechtswidrige Inhalte im Internet vorzugehen, darunter beispielhaft die Verpflichtung von Hostingdiensten und Online-Plattformen ein Meldesystem auf den Diensten einzurichten, über das rechtswidrige Inhalte den Diensteanbietern gemeldet werden können.

Stellen Nutzende, Einrichtungen, Organisationen oder Vereinigungen, die mit der Wahrnehmung der nach dem DSA übertragenen Rechte beauftragt sind, mögliche Verstöße von Diensteanbietern gegen die Vorgaben des DSA fest, so können diese dagegen Beschwerde beim eigenen nationalen DSC einlegen. Wichtig dabei ist, dass es bei der Beschwerde um Verstöße gegen den DSA geht und nicht um identifizierte vermutet rechtswidrige Inhalte an sich. Der DSC nimmt selbst also keine Entfernung von Inhalten oder eine Inhaltskontrolle vor.

Als zentrale Beschwerdestelle prüft der DSC nach Beschwerdeingang zunächst die eigene Zuständigkeit. Im Falle der Zuständigkeit bei einem anderem DSC oder der EU-Kommission, wird die vollständige Beschwerde an die entsprechende Stelle weitergeleitet. Sollte der nationale DSC selbst für die Aufsicht der betroffenen Vermittlungsdienste zuständig sein, so ist er befugt, ein nationales Aufsichtsverfahren gegen den Anbieter des jeweiligen Vermittlungsdienstes einzuleiten.

Durch die EU-Kommission oder andere DSC eingeleitete Verfahren gegen Anbieter von Vermittlungsdiensten unterstützt der nationale DSC auf vorherige Anfrage durch die verfahrensführende Partei zB durch Einholung entsprechender Informationen zum untersuchten Vermittlungsdienst bei nationalen Akteuren und Übermittlung dieser Beiträge.

Als Ergebnis von nationalen und europäischen Aufsichtsverfahren drohen den Anbietern von Vermittlungsdiensten, sofern systematisch gegen den DSA verstoßen wird, empfindliche monetäre Sanktionen.

Der deutsche DSC als Koordinierungsstelle ist dabei nicht alleine für die Umsetzung des DSA in Deutschland zuständig. Aufgrund einer gesetzlichen Aufteilung sind weitere zuständige Behörden die Landesmedienanstalten, die Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) sowie die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI).

Nach über einem Jahr Tätigkeit des DSC kann festgestellt werden, dass die Umsetzung des DSA in Deutschland gut angelaufen ist. Abstimmungen und Austausche mit Marktakteuren haben stattgefunden, Zertifizierungsverfahren wurden abgeschlossen, ein Beschwerdemanagement wurde eingeführt, erste nationale Verfahren begonnen und die EU-Kommission bei den von ihr eingeleiteten Verfahren unterstützt. Für die nächsten Jahre bleibt es für den DSC jedoch weiterhin das Ziel, die eigenen Abläufe zu verbessern und den DSA und dessen Instrumente insbesondere den Nutzenden bekannter zu machen.

Bonn, im August 2025

Dr. Deniz Erdem

ist Referatsleiter im Referat DSC 10 „Grundsatzfragen, Zertifizierungsaufgaben und nationale Koordinierung“ bei der Koordinierungsstelle für digitale Dienste – Digital Services Coordinator (DSC) der BNetzA in Bonn.

Games im neuen Plattformrecht der EU

Eine Einordnung unter dem Digital Services Act

Verbraucherschutz

Digitale Spiele haben sich in den vergangenen Jahren zu komplexen sozialen Angeboten entwickelt, auf denen Spielerinnen und Spieler Inhalte erstellen, kommunizieren und interagieren können. In diesem Beitrag wird die Einordnung solcher Online-Spiele unter den Digital Services Act untersucht. Zugleich gibt

der Beitrag einen Ausblick auf die sich ergebenden Pflichten und Herausforderungen für Spieleanbieter. Insbesondere für Online-Plattformen sind diese herausfordernd.

Lesedauer: ●● Minuten

I. Einleitung

Mit dem Digital Services Act¹ (DSA) betrat die EU Neuland in der Regulierung digitaler Dienste. Dieses umfassende Regelwerk zielt darauf ab, ein sichereres und transparenteres Online-Umfeld zu schaffen und legt dabei besonderen Wert auf den Schutz der Verbraucher und die Wahrung ihrer Grundrechte im digitalen Raum.² Online-Spiele stehen vor neuen rechtlichen Herausforderungen.³ Sie ermöglichen es Spielern oft, auf einfache Weise miteinander in Kontakt zu treten und sich kreativ auszuleben.⁴ Damit fallen sie ggf. in den Geltungsbereich des DSA. Worauf es dabei ankommt, untersuchen wir im Folgenden.

II. Geltungsbereich

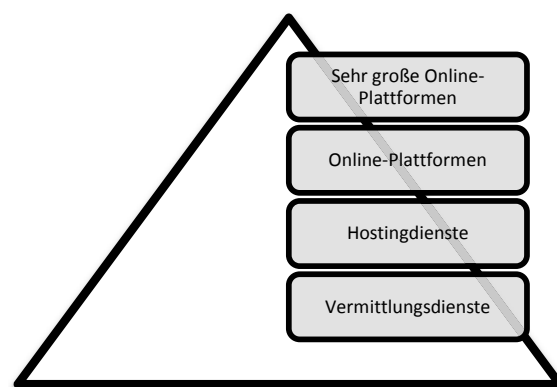
Der DSA enthält harmonisierte Vorschriften für die Erbringung von Vermittlungsdiensten in der Europäischen Union (Art. 2 Abs. 2 DSA). Dabei hängen die anwendbaren Vorschriften und insbesondere die Sorgfaltspflichten von Beschaffenheit, Umfang und Art des Vermittlungsdienstes ab.⁵

Vermittlungsdienste lassen sich gem. Art. 3 lit. g DSA in die folgenden drei unterschiedlichen Kategorien einordnen:

- Dienste der reinen Durchleitung,
- Caching-Leistungen und
- Hosting-Dienste.

Zusätzlich stellt der DSA die Online-Plattform als eine spezielle Form des Hosting-Dienstes heraus (Art. 3 lit. i DSA). Weitergehende Verpflichtungen gelten für sehr große Online-Plattformen (Very Large Online Platforms – VLOPs) – und sehr große Online-Suchmaschinen (Very Large Online Search Engines – VLO-

SEs). Dabei handelt es sich um Dienste, die im Durchschnitt monatlich mind. 45 Mio. aktive Nutzer in der EU haben und von der EU-Kommission als solche benannt wurden (Art. 33 Abs. 1 DSA). Bislang wurde noch kein Online-Spiel als sehr große Online-Plattform benannt.



1. Online-Spiele als Vermittlungsdienste

Auf Online-Spiele ist der DSA nur dann anzuwenden, wenn sie „Vermittlungsdienste“ sind.

a) Dienst der Informationsgesellschaft

Erste Anforderung an einen Vermittlungsdienst ist gem. Art. 3 lit. g DSA, dass es sich um eine Dienstleistung der Informationsgesellschaft (Art. 3 lit. a DSA) handelt. Durch den Verweis des Art. 3 lit. a DSA auf Art. 1 Abs. 1 lit. b RL 2015/1535/EU⁶ wird der Anwendungsbereich auf kommerzielle Dienste, die „idR gegen Entgelt erbracht“ werden, beschränkt.⁷ Die Anforderungen an die Entgeltlichkeit sind in der Praxis gering.⁸ Online-Spiele, die meist durch den Kauf, durch Abogebühren, In-Game-Käufe oder Werbung finanziert werden,⁹ fallen regelmäßig unter diese Begriffsbestimmung.¹⁰

b) Mittlerfunktion

Weiteres zentrales Merkmal eines Vermittlungsdienstes ist seine Rolle als Mittler von Informationen, die von Dritten bereitgestellt werden, ohne dass der Diensteanbieter eine Kontrolle über diese Informationen ausübt.¹¹ Das Verständnis des DSA ist dabei sehr weit. Dies zeigt sich am Begriff der „rechtswidrigen Inhalte“ (Art. 3 lit. h DSA), der Informationen unabhängig von ihrer Form umfasst, solange sie potenziell rechtswidrig sein oder mit rechtswidrigen Handlungen in Zusammenhang stehen können.¹² Für den Bereich der Online-Spiele bedeutet dies, dass Spiele, die den Nutzern Möglichkeiten zur Interaktion und Kreation zur Verfügung stellen, potenziell als Vermittlungsdienste eingestuft werden können, unabhängig davon, ob dies durch das Hochladen von Inhalten, die Eingabe von Texten oder durch spielerische Elemente wie einen umfangreichen Level-Editor geschieht.

¹ VO (EU) 2022/2065 des Europäischen Parlaments und des Rates v. 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der RL 2000/31/EG (Gesetz über digitale Dienste), ABl. 2022 L 277, 1.

² Erwägungsgrund 9 S. 1 DSA.

³ Trunk SpoPrax 2023, 329 (330); Ziff. 46 und 47 der Entschließung des Europäischen Parlaments v. 18.1.2023 zum Binnenmarktkonzept für den Verbraucherschutz in Online-Videospielen (2022/2014(INI)), ABl. 2023 C 214, 15.

⁴ Ziff. 29 der Entschließung des Europäischen Parlaments v. 18.1.2023 zum Binnenmarktkonzept für den Verbraucherschutz in Online-Videospielen (2022/2014(INI)), ABl. 2023 C 214, 159.

⁵ Erwägungsgrund 41 S. 1 DSA.

⁶ RL (EU) 2015/1535 des Europäischen Parlaments und des Rates v. 9.9.2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. 2015 L 241, 1.

⁷ Raue/Heesen NJW 2022, 3537.

⁸ Vgl. Schmidt/Dreyer/Lampert, Spielen im Netz, 2008, S. 64, abrufbar unter: <https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/a/d9293711df7ed3b6f4c4088d9e45dacc5559969.pdf>.

⁹ Hentsch/Falk, Games und Recht/Anderie, ●●● Aufl o Jahr ergänzen ●●● § 17 Rn. 21–26.

¹⁰ Trunk SpoPrax 2023, 329; s.a. für den deutschen Begriff des Telemediums: Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG/Mankowski, 3. Aufl. 2016, S12 Rn. 163a.

¹¹ Hofmann/Raue, Digital Services Act/F. Hofmann, ●●● Auflage und/oder Jahr ergänzen ●●● Art. 3 Rn. 45.

¹² Erwägungsgrund 12 S. 3 DSA.

c) Reine Durchleitung

Bei einer „reinen Durchleitung“ werden Informationen, die von Nutzern bereitgestellt wurden, lediglich über ein Kommunikationsnetz übermittelt (Art. 3 lit. g sublit. i 1. Alt. DSA). Es handelt sich hierbei um einen rein technischen Vorgang der Informationsübertragung. Der Anbieter steht bei dieser Übertragung nicht mit den Inhalten in Verbindung und ändert diese nicht.¹³

d) Hosting-Dienst

Einen Hosting-Dienst zeichnet dadurch aus, dass er von einem Benutzer bereitgestellte Informationen in dessen Auftrag speichert (Art. 3 lit. g sublit. iii DSA).

e) Online-Plattform

Erfüllt der Dienst die Voraussetzungen eines Hosting-Dienstes, stellt sich in der Folge die Frage, ob es sich um eine Online-Plattform handelt, was weitere, umfangreiche Pflichten mit sich bringt. Eine Online-Plattform ist legaldefiniert als „Hosting-Dienst, der im Auftrag eines Nutzers Informationen speichert und öffentlich verbreitet, sofern es sich bei dieser Tätigkeit nicht nur um eine unbedeutende und reine Nebenfunktion eines anderen Dienstes oder um eine unbedeutende Funktion des Hauptdienstes handelt, die aus objektiven und technischen Gründen nicht ohne diesen anderen Dienst genutzt werden kann, und sofern die Integration der Funktion der Nebenfunktion oder der unbedeutenden Funktion in den anderen Dienst nicht dazu dient, die Anwendbarkeit dieser Verordnung zu umgehen“ (Art. 3 lit. i DSA).

Vereinfacht ausgedrückt speichert und verbreitet eine Online-Plattform iSd Art. 3 lit. i DSA die von einem Nutzer bereitgestellten Informationen öffentlich im Auftrag des Nutzers, wobei diese Funktion nicht nur untergeordneter Natur sein darf.

Art. 3 lit. k DSA definiert die Verbreitung an die Öffentlichkeit als Bereitstellung von Informationen für eine potenziell unbegrenzte Anzahl von Dritten auf Anfrage des Empfängers des Dienstes, der die Informationen bereitstellt. Es genügt, dass die Informationen einer potenziell unbegrenzten Zahl von Nutzern leicht zugänglich sind, unabhängig davon, ob auf sie zugegriffen werden.¹⁴ Die Notwendigkeit eines Log-ins ist unschädlich, wenn die Registrierung automatisch erfolgt, dh grundsätzlich jedem offensteht.¹⁵ Viele Online-Spiele ermöglichen eine solche automatische Registrierung, was auf die Erfüllung des Merkmals der Öffentlichkeit hindeutet. Eine öffentliche Verbreitung liegt dann nahe, wenn etwa nutzergenerierte Inhalte innerhalb des Spiels für andere Nutzer sichtbar gemacht werden können.

Einschränkend ist zu prüfen, ob die öffentliche Verbreitung im Gesamtkontext nur eine untergeordnete Rolle spielt. Hierdurch soll eine Überregulierung vermieden werden.¹⁶ Die Entscheidung über die Anwendung dieser Ausnahme erfordert eine Einzelfallbetrachtung, wobei der DSA den rechtlichen Rahmen nur grob konturiert. Der Kommentarbereich einer Online-Zeitung soll als Nebenfunktion angesehen werden, da er klar der Hauptdienstleistung – der Veröffentlichung von Nachrichten unter redaktioneller Verantwortung des Herausgebers – untergeordnet ist.¹⁷ Im Gegensatz dazu soll die Speicherung von Kommentaren in einem sozialen Netzwerk als integraler Bestandteil einer Online-Plattform angesehen werden, da sie offensichtlich keine Nebenfunktion des angebotenen Dienstes darstellt, selbst wenn sie den Beiträgen der Nutzer des Dienstes dient.

2. Bewertung einzelner Spielelemente

Die nachfolgende nicht abschließende (teils technische) Einordnung konzentriert sich auf die spezifischen Eigenschaften und Interaktionsmöglichkeiten, die in Online-Spielen häufig enthalten sind.

a) Chat-Funktionen

Kommunizieren Spieler über Sprach- oder Textkanäle im Spiel miteinander, vermittelt der Anbieter fremde Nutzerinformationen. Diese Funktionen können u.a. als Dienste der reinen Durchleitung oder als Hosting-Dienste klassifiziert werden, abhängig davon, wie die Kommunikation technisch erfolgt.

Der DSA zählt sowohl Sprachtelefonie als auch interpersonelle Kommunikationsdienste als „reine Durchleitung“. Interpersonelle Kommunikationsdienste iSv Art. 2 Nr. 5 Richtlinie über den europäischen Kodex für die elektronische Kommunikation (EKfEK-RL) zeichnet aus, dass sie einen direkten und interaktiven Informationsaustausch zwischen einer endlichen Zahl von Personen ermöglichen, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind. Neben Gruppenchats nennt die EKfEK-RL in Erwägungsgrund 17 EKfEK-RL auch Kommunikationskanäle in Online-Spielen.

Werden die Chats gespeichert, kommt eine Einordnung als Hosting-Dienst (Art. 3 lit. g sublit. iii DSA) in Betracht. Das Speichern von Chats führt bei Online-Spielen jedoch regelmäßig nicht zu einer Einordnung als Online-Plattform gem. Art. 3 lit. i DSA, da die Chats meist nicht öffentlich verbreitet werden. Eine solche Verbreitung würde das Bereitstellen von Informationen für eine unbegrenzte Zahl von Dritten beinhalten, was bei interpersoneller Kommunikation zwischen begrenzten Nutzergruppen nicht der Fall ist.¹⁸ Eine öffentliche Verbreitung kann zB bei öffentlichen Gruppen oder offenen Kanälen vorliegen.¹⁹

b) Gameplay

Auch bei der Teilnahme an einem Online-Spiel findet eine Übermittlung von Informationen an Mit- bzw. Gegenspieler statt. So wird zB beim Online-Schach der Zug eines Spielers über den Server an den Gegenspieler übermittelt. In einem Online-Shooter müssen hingegen in Echtzeitdaten wie die Position, der Zustand (zB Lebenspunkte, Ausrüstung) und die Aktionen (zB Schüsse, Bewegungen) aller Spieler über den Server synchronisiert und an die jeweiligen Clients der Mitspielenden übermittelt werden. Es stellt sich die Frage, ob das Gameplay selbst zu einer Einordnung des Online-Spiels als Vermittlungsdienst führt. Holznagel spricht sich für eine solche Einordnung auch bei einem bloß flüchtigen Spielverlauf aus, da selbst Handlungen wie etwa Beleidigungen kurzzeitig auf den Online-Servern gespeichert werden müssen.²⁰ Diese Auffassung lässt in ihrer Pauschalität allerdings eine genauere Betrachtung der einzelnen technischen Funktionen vermissen.

Wie bereits ausgeführt, kommen bestimmte Kommunikationskanäle wie die Internettelefonie ohne eine flüchtige Speicherung der Nutzerinformationen aus. Zudem liegt nach Auffassung der Verfasser im bloßen Spielen eines Spiels noch keine Speicherung bzw. Verbreitung fremder Nutzerinformationen, wie vom DSA gefordert: Von den Diensten zum Austausch von Informationen und Inhalten, die der Gesetzgeber mit Erwägungsgrund 29 S. 4 DSA im Sinn hatte, scheint eine Online-Sportsimulation oder ein rein kompetitiver Battle-Royal-Shooter weit entfernt. Was im Spielverlauf möglich ist und was nicht, ist durch das Spielprogramm konkret festgelegt.

¹³ Gersdorf/Paal, BeckOK Informations- und Medienrecht/Hennemann, 46. Aufl. 2023, TMG § 8 Rn. 14.

¹⁴ Erwägungsgrund 14 S. 1 DSA.

¹⁵ Erwägungsgrund 14 S. 2 DSA.

¹⁶ Erwägungsgrund 13 S. 3 DSA.

¹⁷ Erwägungsgrund 13 S. 4 und 5 DSA.

¹⁸ Erwägungsgrund 14 S. 3 DSA.

¹⁹ Erwägungsgrund 14 S. 4 DSA.

²⁰ Müller-Terpitz/Köhler, DSA/Holznagel, Art. 3 Rn. 89.

Eine Einordnung als Vermittlungsdienst ist iÜ auch nach Wortlaut und Telos nicht geboten. Der Begriff der „Information“, der für die Eröffnung des Anwendungsbereichs maßgeblich ist, ist weder im DSA noch in der E-Commerce-Richtlinie²¹ legaldefiniert. Auch in der englischen²² und französischen²³ Fassung fehlen Anhaltspunkte für dessen unionsrechtliche Wortbedeutung. Der DSA legt jedoch einen Unterschied zwischen „Information“ und „Inhalten“ nahe, da er beide Begriffe zB in der Begriffsbestimmung über die „Moderation von Inhalten“ verwendet. Vergleicht man den DSA mit anderen Digitalrechtsakten wie dem Data Act²⁴, erscheint der Begriff „Information“ weniger umfassend als der Begriff „Daten“.²⁵ Dabei ist jedoch zu berücksichtigen, dass der Data Act mit dem fairen Zugang zu Daten ein anderes Ziel verfolgt als der DSA, was gegen ein einheitliches Begriffsverständnis sprechen könnte.²⁶ Betrachtet man den Sinn und Zweck des DSA, so zielt dieser auf ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld, das der Verbreitung rechtswidriger Online-Inhalte und gesellschaftlicher Risiken, wie der Desinformation, entgegenwirkt.²⁷ Diese Risiken lassen sich auf vorprogrammierte Spielinteraktionen grundsätzlich nicht übertragen: Die spielerischen Möglichkeiten sind in den meisten Online-Spielen durch das Computerprogramm so begrenzt, dass (rechtswidrige) Inhalte oder Informationen, die der DSA adressiert, aus dem bloßen Spielverlauf regelmäßig nicht entstehen können. Insoweit ist das Spielen selbst eher mit einem interaktiven Film (zB Black Mirror: Bandersnatch²⁸) vergleichbar. Wäre das Begriffsverständnis des DSA so weit, dass bereits das Drücken eines Knopfes oder eine simple Auswahlmöglichkeit vorconfigurierter Optionen, eine vom Nutzer bereitgestellte Information iSd DSA ist, müsste auch jedes Abspeichern von Einstellungen in einem Online-Dienst zu einer Einordnung als Hosting-Dienst führen. Dies würde zu einer erheblichen Überregulierung führen, deren Sinnhaftigkeit zweifelhaft ist.

c) Nutzergenerierte Inhalte und virtuelle Identitäten

Online-Spiele bieten häufig kreative Freiheiten in Form der Möglichkeit von nutzergenerierten Inhalten. Diese reichen von der Gestaltung des Avatars oder der Fahrzeugkarosserie bis hin zur Schöpfung ganzer Spielwelten. Zudem haben Nutzer oft die

Möglichkeit, ihr Profil mit einem individuell gewählten Nutzernamen und ggf. weiteren Informationen wie Texten zu personalisieren. Manche Spiele ermöglichen es auch, dass Nutzer eigene Logos entwerfen, die im Spiel sichtbar sind.²⁹ Diese Inhalte können gesetzeswidrig sein oder im Widerspruch zu den Regeln aus dem Spielnutzungsvertrag mit dem Publisher stehen. Durch die Speicherung dieser Inhalte erbringt der Publisher idR einen Hosting-Dienst gem. Art. 3 lit. g sublit. iii DSA.

d) Gesamtwürdigung

Wenn nach den oben dargestellten Kriterien eine öffentliche Verbreitung von Informationen vorliegt, die von Nutzern bereitgestellt wurden, liegt eine Online-Plattform vor, sofern es sich dabei nicht um eine untergeordnete Nebenfunktion handelt. In diesem Zusammenhang ist zu ermitteln, was die Hauptfunktion des Dienstes ist.

Online-Spiele dienen üblicherweise dazu, gemeinsam an dem Spielerlebnis zu partizipieren. In kompetitiven Spielen geht es vor allem darum, miteinander in den Wettkampf zu treten, während in story-basierten Rollenspielen das (häufig gemeinsame) Lösen von Aufgaben und das Erleben der Geschichte zentral sind. Die Spielfunktionen können dabei so umfangreich wie vielfältig sein. Allerdings stehen in manchen Online-Spielen wie Roblox³⁰ oder Minecraft³¹ nutzergenerierte Inhalte deutlich mehr im Vordergrund. In diesen Spielen können Nutzer ganze Welten kreieren und mit anderen Nutzern teilen. Je stärker der Fokus auf diesen Funktionen liegt, desto geringer ist der argumentative Spielraum gegen eine Einordnung als Online-Plattform.

III. Sorgfaltspflichten unter dem DSA

Die Sorgfaltspflichten des DSA können in ihrer Detailliertheit ganze Buchkapitel oder sogar Bücher füllen. Im Folgenden soll daher vor allem auf die Eigenarten von Online-Spielen eingegangen werden.

Für ein erstes Verständnis ist es hilfreich, sich zu vergegenwärtigen, dass der DSA grundlegende Pflichten für alle Anbieter von Vermittlungsdiensten und zusätzliche Pflichten für Anbieter von Hosting-Diensten, insbesondere für Anbieter von Online-Plattformen und sehr großen Online-Plattformen (VLOPs), festlegt. Die in diesem Abschnitt erläuterten Sorgfaltspflichten sind nicht abschließend zu verstehen.

1. Allgemeine Geschäftsbedingungen

Eine zentrale Forderung des DSA ist die Transparenz bei der Beschränkung von Inhalten durch den Vermittlungsdienst. Als eine der wesentlichen Informationsquellen in Bezug auf die Beschränkungen identifiziert der DSA die Allgemeinen Geschäftsbedingungen (AGB) der Vermittlungsdienste.³² In diesen müssen nach Art. 14 DSA ungeachtet von Art und Größe des Vermittlungsdienstes bestimmte Parameter über die Moderation von Inhalten offengelegt werden. Anders als bei anderen Pflichten wie dem Erfordernis jährlicher Transparenzberichte (Art. 15 DSA) besteht keine Ausnahme für Klein- oder Kleinstunternehmen.³³

Die Moderation von Inhalten beschreibt die – automatisierten oder nicht-automatisierten – Tätigkeiten, mit denen insbesondere rechtswidrige oder mit den AGB unvereinbare Inhalte oder Informationen, die von Nutzern bereitgestellt werden, festgestellt und bekämpft werden sollen (Art. 3 lit. t DSA). Darunter fallen Maßnahmen, die sich auf Verfügbarkeit, Anzeige und Zugänglichkeit dieser Informationen auswirken.

Viele Online-Spiele enthalten bereits heute Verhaltensregeln in ihren Endnutzerlizenzvereinbarungen³⁴ oder weiteren Leitlinien³⁵. Diese Verhaltensregeln können als AGB einzuordnen sein.³⁶ Der DSA gibt einen klaren und für Nutzer vorhersehbaren

²¹ RL (EG) 2000/31 des Europäischen Parlaments und des Rates v. 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr), ABl. 2000 L 178, 1.

²² Information provided by the recipient of the service.

²³ Informations fournies par un destinataire du service.

²⁴ VO (EU) 2023/2854 des Europäischen Parlaments und des Rates v. 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der VO (EU) 2017/2394 und der RL (EU) 2020/1828 (Datenverordnung), ABl. 2023 L, 2023/28549.

²⁵ Daten sind in Art. 2 Nr. 1 DA definiert als „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material“.

²⁶ Erwägungsgrund 5 DA.

²⁷ Erwägungsgrund 9 S. 1 DSA.

²⁸ „Black Mirror: Bandersnatch“ ist ein auf Netflix veröffentlichter Film, in dem Zuschauer mehrfach durch Selektionsentscheidungen die Richtung der Handlung bestimmen können.

²⁹ Ein bekanntes Beispiel ist der Emblem-Generator, der u.a. in verschiedenen Spielen von Call of Duty oder in Armored Core VI™; Fires of Rubicon™ zu finden ist.

³⁰ Roblox ist eine von Roblox Corporation entwickelte Spieleplattform.

³¹ Minecraft ist ein Sandbox-Computerspiel, das von Mojang Studios entwickelt wurde.

³² Hofmann/Raue, Digital Services Act/F. Hofmann, ●●● Art. 1 Rn. 22.

³³ ZB Art. 15 Abs. 2 DSA.

³⁴ Maties, Stichwortkommentar eSport-Recht/Picot, ●●● Auflage o Jahr ergänzen, S. 48 Rn. 2.

³⁵ ZB der Verhaltenskodex von Rocket League, abrufbar unter: <https://www.rocketleague.com/de/news/rocket-league-code-of-conduct>.

³⁶ BGH MMR 2017, 394 Rn. 51 f.; Hentsch/Falk, Games und Recht/Sestner/Kaster, ●●● § 18 Rn. 22.

rechtlichen Rahmen für die Moderation von Inhalten vor.³⁷ Anbieter müssen daher sicherstellen, dass sie die entsprechenden Informationen in Übereinstimmung mit den Vorgaben des DSA bereitstellen.

Problematisch sind unbestimmte Formulierungen in AGB wie nicht abschließende Aufzählungen bei Verboten. Diese Redewendungen bieten Anbietern unter dem DSA keinen Mehrwert, da sie alle Beschränkungen offenlegen sollen, eine willkürliche Moderation nicht geregelter Fälle grundsätzlich unterbleiben soll.³⁸ Abstraktere Begriffe wie Hassrede können zulässig sein, insbesondere wenn diese mit Beispielen unterlegt sind.³⁹ Spezifische Fachtermini, die bei der Zielgruppe bekannt sind, dürfen verwendet werden,⁴⁰ jedoch sollten weniger geläufige Begriffe für ein breites Publikum verständlich erläutert werden.

Der DSA verpflichtet zu Angaben über Maßnahmen und Werkzeuge, mit denen unerwünschte Inhalte erkannt und festgestellt werden können. Dies umfasst die menschliche Überprüfung, ebenso wie Werkzeuge, die zur automatisierten Moderation von Inhalten eingesetzt werden. Auch einfache Lösungen wie Wortfilter, die gemäß einer Liste des Publishers zB Schimpfwörter im Chat unterdrücken, können als Werkzeuge betrachtet werden. Das Melde- und Abhilfeverfahren, das der DSA in Art. 16 DSA vorsieht, kann ebenfalls als Instrument zur Beschränkung von Inhalten verstanden werden.⁴¹

Für Anti-Cheat-Maßnahmen sieht der DSA keine näheren Angaben zu Werkzeugen vor. Beim Cheaten manipuliert der Cheater idR den Programmablauf und verschafft sich dadurch einen spielerischen Vorteil,⁴² indem er zB automatisch zielen⁴³ oder durch Wände sehen kann⁴⁴. Eigene Informationen idS DSA stellen Spieler durch das bloße Spielen unter Zuhilfenahme von Cheats aber meist nicht bereit (s. unter II.2.b)).

2. Transparenzberichte

Alle Dienstleister sind verpflichtet, mindestens einmal jährlich einen Transparenzbericht zu veröffentlichen, es sei denn, sie gelten als Kleinst- oder Kleinunternehmen (Art. 15 Abs. 1 S. 1 DSA). Diese Transparenzberichte müssen Angaben zu den bei ihnen eingegangenen behördlichen Anordnungen (lit. a), aussagekräftige und unter nachvollziehbare Informationen über die in Eigenregie durchgeführte Inhaltsmoderation (lit. c) und die Anzahl der über die internen Beschwerdemanagementsysteme eingegangenen Beschwerden gemäß den AGB des Diensteanbieters (lit. d) enthalten. Anbieter von Hosting-Diensten, Online-Plattformen und sehr großen Online-Plattformen sind zu weitergehenden Angaben in ihren Transparenzberichten verpflichtet.

Die EU-Kommission hat eine Durchführungsverordnung gem. Art. 15 Abs. 3 DSA erlassen, um ein verbindliches Muster für die Form und den Inhalt der Transparenzberichte festzulegen und die Berichtszeiträume zu harmonisieren.⁴⁵ Diese sind für die meisten Online-Spiele erkennbar unangemessen.

3. Melde- und Abhilfeverfahren für Hosting-Dienste

Anbieter von Hosting-Diensten und damit auch Online-Plattformen müssen unabhängig von ihrer Größe ein leicht zugängliches und benutzerfreundliches Melde- und Abhilfeverfahren einrichten, das es Personen und Einrichtungen ermöglicht, Informationen zu melden, die sie für rechtswidrig halten (Art. 16 Abs. 1 DSA). Viele Details sind in Art. 16 DSA geregelt. U.a. soll das Verfahren für jedermann leicht zugänglich sein, also nicht nur für Nutzer, sondern auch für Dritte, zB Behörden.⁴⁶ Da die Meldefunktion auch in unmittelbarer Nähe der ggf. zu meldenden Information liegen soll,⁴⁷ sind die Anforderungen für Online-Spiele nicht ohne Weiteres zu erfüllen, weil ein Widerspruch zwischen der Anforderung, dass die Meldemöglichkeit in der Nähe zu der

meldenden Information (also Meldemöglichkeit direkt im Spiel) und der freien Zugänglichkeit für alle (also ohne Anmeldung) besteht. Um Zugang zum Spiel (und damit einem Melde- und Abhilfeverfahren in unmittelbarer Nähe der ggf. problematischen Information) zu erhalten, benötigt jeder Nutzer grundsätzlich eine entsprechende Lizenz, die in der Praxis idR eine Registrierung (und/oder den Abschluss eines Spielnutzungsvertrags) voraussetzt. Es zeigt sich, dass die Besonderheiten, die bei Online-Spielen zu berücksichtigen sind, durch die recht starren Vorgaben des Art. 16 DSA nicht angemessen berücksichtigt werden.

4. Empfehlungssysteme

Anbieter von Online-Plattformen, die sog. Empfehlungssysteme verwenden, müssen in ihren AGB in klarer und verständlicher Sprache die wesentlichen Parameter dieser Systeme sowie alle Möglichkeiten der Nutzer, diese wesentlichen Parameter zu ändern oder zu beeinflussen, darlegen (Art. 27 Abs. 1 DSA). Empfehlungssysteme, genauer definiert in Art. 3 lit. s DSA, sind Filterwerkzeuge, die den Nutzern helfen sollen, die ihnen präsentierten Inhalte zu priorisieren.⁴⁸ Bei Online-Spielen ist dies zB dann relevant, wenn in einem Katalog verschiedene nutzergenerierte Inhalte vorgeschlagen werden. Durch die Transparenzpflicht soll der Nutzer darüber informiert werden, warum ihm bestimmte nutzergenerierte Inhalte angeboten werden.

5. Offenlegung der aktiven Nutzer

Neben anderen Transparenzberichtspflichten sind Online-Plattformen verpflichtet, mindestens halbjährlich die durchschnittliche Zahl ihrer monatlich aktiven Nutzer in der Union zu veröffentlichen (Art. 24 Abs. 2 DSA). Diese Kennziffer ist relevant, da Online-Plattformen mit mehr als 45 Mio. aktiven Nutzern als VLOPs einer Vielzahl weiterer Sorgfaltspflichten und der Aufsicht durch die EU-Kommission unterliegen. Die Zahl der aktiven Nutzer im Monatsdurchschnitt sollte alle Nutzer widerspiegeln, die den Dienst mindestens einmal tatsächlich genutzt haben, indem sie den über die Online-Schnittstelle der Online-Plattform verbreiteten Informationen ausgesetzt waren, zB durch Ansehen, Anhören oder Bereitstellen von Informationen.⁴⁹ Eine zuverlässige Ermittlung dieser Zahlen ist wegen der datenschutzrechtlichen Vorgaben über Nutzer-Tracking generell schwierig. Besteht ein Spiel aus mehreren unterschiedlichen Komponenten, von denen nicht alle als Online-Plattform zu klassifizieren sind, sprechen aus Sicht der Autoren gute Argumente dafür, die Anzahl dieser Nutzer und nicht die Gesamtzahl aller aktiven Spieler des Spiels als relevanten Maßstab heranzuziehen. In diesem Fall sind nämlich auch nur diejenigen Spieler Informationen der Online-Plattform ausgesetzt, die die jeweilige Spielkomponente genutzt haben, sodass für die anderen Spieler kein Risiko von potenziell rechtswidrigen Drittinhalten ausgeht.

³⁷ Erwägungsgrund 47 S. 1 DSA; Raue/Heesen NJW 2022, 3537 (3540).

³⁸ Hofmann/Raue, Digital Services Act/Raue, ●●● Art. 14 Rn. 3; Schwartmann NJW 2022, 133 (134); Raue/Heesen NJW 2022, 3537 (3540).

³⁹ OLG Dresden MMR 2018, 756 Rn. 13 ff.

⁴⁰ BGH MMR 2017, 394 Rn. 63; Trunk SpoPrax 2022, 216 (218); Maties/Püschel SpoPrax 2022, 306 (308).

⁴¹ Ziff. 8 der ZeniMax Media-Nutzungsbedingungen, abrufbar unter: <https://www.zenimax.com/de/legal/terms-of-service>.

⁴² Nothelfer/Trunk SpoPrax 2022, 341.

⁴³ Sog. Aim-Bots.

⁴⁴ Sog. Wall- oder Map-Hacks.

⁴⁵ Durchführungsverordnung (EU) 2024/2835 der Kommission v. 4.11.2024 zur Festlegung von Vorlagen für die Transparenzberichtspflichten der Anbieter von Vermittlungsdiensten und der Anbieter von Online-Plattformen gemäß der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates. ABl. L, 2024/2835.

⁴⁶ Spindler GRUR 2021, 545 (552); Hoffmann/Raue, Digital Services Act/Raue, ●●● Art. 16 Rn. 16.

⁴⁷ Erwägungsgrund 53 S. 3 DSA.

⁴⁸ Hofmann/Raue, Digital Services Act/Grise, ●●● Art. 27 Rn. 13.

⁴⁹ Erwägungsgrund 77 S. 2 DSA.

5. Minderjährige

Der DSA sieht an mehreren Stellen besondere Vorschriften zum Schutz Minderjähriger vor. Diese werden in Deutschland von der Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten (KidD) durchgesetzt, die bei der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) angesiedelt ist.⁵⁰ Richtet sich ein Vermittlungsdienst in erster Linie an Minderjährige oder wird er überwiegend von diesen genutzt, so hat der Anbieter die Bedingungen und Beschränkungen für die Nutzung des Dienstes in einer für Minderjährige verständlichen Form zu erläutern (Art. 14 Abs. 3 DSA). Davon kann ausgegangen werden, wenn mehr als 50% der Nutzer minderjährig sind.⁵¹ Die Anbieter können in Erwägung ziehen, in ihren Bedingungen grafische Elemente wie Icons oder Bilder zu verwenden, um die wesentlichen Elemente der Informationspflichten zu veranschaulichen.⁵²

Online-Plattformen, die für Minderjährige zugänglich sind, müssen geeignete und verhältnismäßige Maßnahmen ergreifen, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz für Minderjährige in ihrem Dienst zu gewährleisten (Art. 28 Abs. 1 DSA).⁵³ Gezielte Werbung gegenüber Minderjährigen ist verboten (Art. 28 Abs. 2 DSA), dh – im Gegensatz zur DS-GVO – nicht einmal auf der Grundlage einer Einwilligung erlaubt.

IV. Ausblick

Die Einführung des DSA stellt Anbieter von Online-Spielen vor neue rechtliche Herausforderungen. Aufgrund ihrer interaktiven und sozialen Natur können diese in den Anwendungsbereich des DSA fallen, insbesondere wenn sie nutzergenerierte Inhalte speichern und mit anderen Spielern teilen. Dies kann eine kleinteilige Überprüfung und ggf. Anpassung des Spiels erfordern, um den neuen rechtlichen Anforderungen gerecht zu werden. Derartige Anforderungen gehen immer mit einem großen

⁵⁰ S. hierzu Terhörst MMR 2024, 525.

⁵¹ Kraul, Das neue Recht der digitalen Dienste/Maamar, ●●● Aufl. o Jahr ergänzen ●●● § 4 Rn. 43; Hofmann/Raue, Digital Services Act/Raue, ●●● Art. 14 Rn. 70.

⁵² Erwägungsgrund 45 S. 5 DSA.

⁵³ S.a. von Petersdorff MMR 2025, ●●● – in diesem Heft.

Mehraufwand einher, der insbesondere kleinere Spieleanbieter vor wirtschaftliche Herausforderungen stellt. Zugleich existieren bei einigen Sorgfaltspflichten noch keine klaren, verbindlichen Vorgaben, wie diese in Online-Spielen sinnvoll (!) zu realisieren sind. Mit Spannung bleibt daher abzuwarten, wie die Umsetzung durch Anbieter aber auch die Überwachung durch Behörden in den nächsten Monaten und Jahren erfolgt. Letztlich wird der Erfolg des DSA gerade daran gemessen werden, inwiefern er in den EU-Mitgliedstaaten durchgesetzt wird.

Schnell gelesen ...

- Die Einordnung von Online-Spielen unter dem DSA hängt von deren Features und der technischen Umsetzung ab. Untersucht werden sollten insbesondere Spiele mit Interaktionsmöglichkeiten wie Kommunikation und Nutzerinhalten.
- Anders als Chats oder nutzergenerierte Inhalte stellen die Aktionen des Spielers im normalen Spielverlauf nach der hier vertretenen Auffassung idR keine „fremde Information“ dar, die der Spieleanbieter vermittelt.
- Die Sorgfaltspflichten unter dem DSA stellen Publisher vor neue Herausforderungen. Handlungsbedarf besteht u.a. bei den AGB.
- Die Vorgaben für das Melde- und Abhilfeverfahren bei Hosting-Diensten passen nur bedingt bei Online-Spielen.



Dr. Andreas Lober

ist Rechtsanwalt und Partner bei ADVANT Beiten in Frankfurt/M. und Leiter der Praxisgruppe IP/IT/Medien.



Daniel Trunk

ist Rechtsanwalt bei ADVANT Beiten in Frankfurt/M.

LORENZO VON PETERSDORFF

Online-Schutz Minderjähriger nach dem DSA

Implikationen der EU-Leitlinien für die Games-Branche

Schutzstandards

Mit Art. 28 DSA formuliert die EU erstmals einen strukturellen Schutzrahmen für Minderjährige auf Online-Plattformen. Der aktuelle Leitlinien-Entwurf der EU-Kommission konkretisiert die Pflichten der Anbieter, birgt jedoch in seiner Umsetzung Herausforderungen für Rechtssicherheit und Praktikabilität, auch für die Games-Branche. Der Beitrag gibt einen Überblick zum rechtlichen Rahmen und analysiert aus Perspektive der Unterhaltungssoftware Selbstkontrolle (USK) zentrale Aspekte des Entwurfs, darunter die Grundprinzipien sowie ausgewählte

Maßnahmen. Dabei zeigt sich, dass insbesondere die starke Fokussierung auf technische Altersprüfungen zulasten anderer bewährter Instrumente geht. Fragen im Hinblick auf die Systematik, unklare Begrifflichkeiten und der Eindruck faktischer Verpflichtungen erschweren eine kohärente Umsetzung. Der Beitrag plädiert für eine risikoorientierte, verhältnismäßige Anwendung unter Einbindung bewährter und bereits bestehender (selbstregulatorischer) Ansätze. **Lesedauer: ●● Minuten**

I. Einleitung

Der Schutz von Minderjährigen ist ein wichtiges politisches Ziel der EU.¹ Dies manifestiert sich zentral durch die Regelung des Art. 28 VO (EU) 2022/2065 (DSA), die den Kinder- und Jugend-

schutz auf Ebene der Plattformregulierung verankert. Online-Plattformen sind zu zentralen Erfahrungs- und Kommunikationsräumen für Minderjährige geworden. Sie bieten einerseits Zugang zu Bildungsangeboten, sozialer Teilhabe und kreativer Entfaltung, bergen aber zugleich eine Vielzahl an Risiken, etwa durch Kommunikations- und Kontaktstrisiken, problematische In-

¹ Vgl. Erwägungsgrund 71 DSA S. 1.

halte, manipulative Designelemente oder durch die Einbindung KI-basierter Interaktionssysteme. Auch im Bereich der Games-Branche existieren relevante Angebote, die dem Begriff der Online-Plattform iSd Art. 3 lit. i DSA unterfallen können.² So sind einige Spieleplattformen schon heute weit mehr als reine Distributoren, sondern ermöglichen auch umfangreiche Möglichkeiten der Interaktion, Kommunikation oder das Erschaffen und Teilen nutzergenerierter Spielwelten, ohne vertiefte Programmierkenntnisse.³ Die Notwendigkeit rechtsverbindlicher Schutzvorkehrungen ergibt sich insbesondere aus den primärrechtlichen Gewährleistungen der GRCh. Minderjährigen steht dabei besondere Berücksichtigung zu, da im Rahmen ihrer Entwicklung zu ausgewachsenen Persönlichkeiten Schutz-, Befähigungs- und Teilhaberechte von besonderer Relevanz sind, wie es auch die 25. Allgemeinen Bemerkung zur UN-Kinderrechtskonvention in digitalen Umgebungen festhält.⁴ Aus Perspektive der Unterhaltungssoftware Selbstkontrolle (USK) als „One-Stop-Shop“ für Jugendmedienschutz im Games-Bereich in Deutschland gibt der vorliegende Beitrag einen Überblick über den rechtlichen Rahmen, die Chancen und Herausforderungen einer differenzierten, risikoorientierten Umsetzung der Sorgfaltspflichten nach Art. 28 Abs. 1 DSA. Im Mittelpunkt steht dabei der aktuelle Entwurf der durch die EU-Kommission veröffentlichten Leitlinien nach Art. 28 Abs. 4 DSA, deren wesentliche Inhalte im Überblick sowie in ausgewählten Aspekten vertiefend dargestellt werden.⁵

II. Systematik des Online-Schutzes Minderjähriger nach dem DSA

Gemäß Absatz 1 des Art. 28 DSA werden Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, dazu verpflichtet, geeignete und verhältnismäßige Maßnahmen zu ergreifen, „um für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen“. Um die Anbieter von Online-Plattformen bei der Anwendung von Absatz 1 und den darin enthaltenen unbestimmten Rechtsbegriffen zu unterstützen kann die Kommission Leitlinien herausgeben (s. unter ●●●). Deutschland hat von der Vorschrift des Art. 49 Abs. 2 UAbs. 1 S. 2 Gebrauch gemacht, sodass die Bundeszentrale für Kinder- und Jugendmedienschutz (BZKJ) bzw. die Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten (KidD) gem. § 12 Abs. 2 DDG zuständige Behörde für die Durchsetzung von strukturellen Vorsorgemaßnahmen nach Art. 28 Abs. 1 DSA ist, soweit diese nicht Maßnahmen nach dem Jugendmedienschutz-Staatsvertrag (JMStV) betreffen⁶. Für diese Maßnahmen sowie für konkrete Einzelmaßnahmen nach dem JMStV sind die Stellen der Länder zuständig. Absatz 2 und 3 enthalten datenschutzrechtliche Vorgaben: Absatz 3 untersagt Plattformen, personalisierte Werbung auf Basis von Profiling (Art. 4 Abs. 4 DS-GVO) an Nutzer auszuspielen, wenn sie mit hinreichender Gewissheit minderjährig sind. Zugleich stellt er klar, dass zur Einhaltung von Art. 28 DSA keine zusätzlichen personenbezogenen Daten zur Altersfeststellung verarbeitet werden dürfen (Datenminimierung, Art. 5 Abs. 1 lit. c DS-GVO). Zuständig ist die Bundesbeauftragte für den Datenschutz (BfDI; § 12 Abs. 3 DDG). Der Grundsatz der Datenminimierung gilt auch für Maßnahmen nach Absatz 1. Altersverifikationssysteme sind daher unzulässig, wenn sie zusätzliche personenbezogene Daten erheben.⁷

1. Normadressat des Art. 28 Abs. 1 DSA

a) Online-Plattform

Art. 28 DSA adressiert Online-Plattformen iSd Art. 3 lit. i DSA und damit eine Unterkategorie der Hosting-Dienste. Anders als „reine“ Hosting-Dienste, die von einem Nutzer bereitgestellte Informationen in dessen Auftrag speichern, zeichnen sich On-

line-Plattformen dadurch aus, dass sie Inhalte bzw. Informationen öffentlich verbreiten. Handelt es sich bei der Speicherung und Verbreitung jedoch lediglich um eine nachrangige Nebenfunktion, liegt keine Online-Plattform vor. Diese in der Praxis wohl bedeutende Rückausnahme ist gegeben, wenn es sich um eine bloße Nebenfunktion eines anderen Dienstes oder eine unbedeutende Funktion des Hauptdienstes handelt, die aus objektiven und technischen Gründen nicht ohne diesen anderen Hauptdienst genutzt werden kann.⁸ Enthalten ist auch ein entsprechendes Umgehungsverbot. Nicht erfasst sind somit Film- und Spielplattformen iSd nationaler Regelung des § 14a JuSchG, sofern der Hauptdienst nicht das Angebot fremder, sondern eigener Inhalte zum individuellen Abruf umfasst (zB Plattformen der Konsolen Playstation, Xbox, Nintendo Switch etc.). Werden von diesen Plattformen neben der Hauptfunktion in Form von umfangreichen eigenen Inhalten nur ergänzende Kommunikationsfunktionen (Spieler-Chat) oder Sharing-Funktionen von geringerem Umfang (zB Game-Snapshot-Sharing) bereitgestellt, so sind die Dienste dennoch nicht als Online-Plattformen zu qualifizieren.⁹ Anders ist dies hingegen bei Angeboten wie der Plattform Roblox zu beurteilen. Keine Anwendung findet die Vorschrift des Art. 28 DSA zudem auf Anbieter von Online-Plattformen, die als Kleinst- oder Kleinunternehmen gemäß der Empfehlung 2003/361/EG zu subsumieren sind.¹⁰ Unabhängig von Größe und Umsatz, fallen sehr große Online-Plattformen (Very Large Online Platforms – VLOPs) iSd Art. 33 DSA gem. Art. 19 Abs. 2 DSA jedoch stets unter die Sorgfaltspflichten.

b) „Für Minderjährige zugänglich“

Gem. Art. 28 Abs. 1 DSA werden nur Online-Plattformen, die „für Minderjährige zugänglich“ sind, von dessen Anwendungsbereich erfasst. Als Minderjährig gelten Personen unter 18 Jahren.¹¹ Gem. Erwägungsgrund 71 DSA fallen Online-Plattformen unter dieses Merkmal, wenn ihre AGB „es Minderjährigen gestatten, den Dienst zu nutzen, wenn ihr Dienst sich an Minderjährige richtet oder überwiegend von Minderjährigen genutzt wird oder wenn dem Anbieter in anderer Weise bekannt ist, dass einige seiner Nutzer minderjährig sind, etwa weil er bereits personenbezogene Daten von Nutzern verarbeitet, aus denen das Alter der Nutzer zu anderen Zwecken hervorgeht.“ Die Formulierung vermittelt den Eindruck, als stünden diese Kriterien alternativ nebeneinander. Dies hätte im Umkehrschluss zur Folge, dass eine Anwendung der Regelung des Art. 28 Abs. 1 DSA et-

² Ausf. Lober/Trunk MMR 2025, ●●● – in diesem Heft.

³ Vgl. PM der USK v. 15.1.2025 zu „Game Creator Plattformen auf dem Prüfstand: Änderung der Alterskennzeichen bei unzureichendem Jugendschutz“, abrufbar unter:

<https://usk.de/game-creator-plattformen-auf-dem-pruefstand-aenderung-der-alt-erkennzeichen-bei-unzureichendem-jugendschutz/>.

⁴ ●●● Mast/Kettemann/Dreyer/Schulz, Digital Services Act, 2024, Art. 28 Rn. 2.

⁵ EU-Kommission, PM v. 13.5.2025 zu den „Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065“ (Leitlinien Entwurf), abrufbar unter: <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>.

⁶ S. hierzu Terhörst MMR 2024, 525.

⁷ BeckOK JugendschutzR/Liesching, 4. Ed. 1.12.2024, DSA Art. 28 Rn. 55.

⁸ Beispiele finden sich in Erwägungsgrund 13 UAbs. 1 S. 4 f. (Kommentarbereich einer Online-Zeitung; Web-Hostig) sowie Gegenbeispiele (Verbreitung von Kommentaren in sozialen Netzwerken).

⁹ BeckOK JugendschutzR/Liesching, 4. Ed. 1.12.2024, DSA Art. 28 Rn. 6.

¹⁰ Die derzeitigen Schwellenwerte sehen für Kleinunternehmen weniger als 50 Beschäftigte und einen Jahresumsatz, der 10 Mio. EUR nicht übersteigt, vor. Für Kleinunternehmen weniger als 10 Beschäftigte und einen Jahresumsatz, der 2 Mio. ●●● nicht übersteigt.

¹¹ Vgl. Klarstellung in Fn. 1 des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU Kommission v. 13.5.2025, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>.

wa schon dann nicht mehr möglich wäre, wenn die AGB der Plattform eine Nutzung erst durch Volljährige zuließen, obwohl die Plattform faktisch überwiegend von Minderjährigen genutzt wird. In Anlehnung an den weiten Wortlaut der Norm, hat die EU-Kommission iRd Leitlinien-Entwurfs gem. Art. 25 Abs. 4 DSA jedoch klargestellt, dass bereits die faktische Möglichkeit des Zugangs zur jeweiligen Online-Plattform genügt, um den Anwendungsbereich zu eröffnen.¹² Angebote, die ausschließlich Erwachsenen zugänglich sind, können in Konsequenz nicht vom Anwendungsbereich erfasst sein, etwa aufgrund dokumentgestützter und personenidentifizierter Altersverifikationen (AVS), wie sie etwa im Rahmen nationalgesetzlicher Jugendschutzstandards gem. § 4 Abs. 2 S. 1 Nr. 1, S. 2 JMStV Anwendung finden.¹³

2. Maßnahmen

Der Begriff der „Maßnahme“ ist iSd Art. 28 DSA weit auszulegen. Er erfasst sämtliche, vorwiegend präventiv wirkende und auf den Dienst bezogene Handlungen, Vorkehrungen und Ausgestaltungen, einschließlich technischer Funktionen, Verfahren und Prozesse oder die Zusammenarbeit mit externen Dritten. Darüber hinaus sind auch Dokumentationsformen oder begleitende informationsbezogene Aktivitäten, wie zB Informationskampagnen oder Evaluationen sowie Maßnahmen, die nach der Realisierung eines Risikos wirken und dieses eindämmen können, erfasst.¹⁴ Nach Art. 28 Abs. 1 DSA sind Maßnahmen geeignet und verhältnismäßig auszugestalten. Dh, sie müssen sich positiv auf die Schutzdimensionen Privatsphäre, Sicherheit und Schutz auswirken und den Aufwand in einem angemessenen Verhältnis zur angestrebten Risikominderung stehen. Je höher das Schadenspotenzial eines Online-Angebots für Minderjährige ist, desto umfassender fallen die zu ergreifenden Schutzmaßnahmen aus. Da verschiedene Online-Plattformen unterschiedliche Risiken für Minderjährige bergen, bedarf stets einer Einzelfallprüfung. Entsprechend des Leitlinien Entwurfs der EU-Kommission sollen dabei die Art und Beschaffenheit der vom Anbieter angebotenen Dienste, die beabsichtigte oder aktuelle Nutzung sowie die Nutzerbasis des Dienstes Berücksichtigung finden. Zudem hat der Anbieter etwaige Grundrechtseingriffe, insbesondere im Hinblick auf die Rechte Minderjähriger nach der GRCh, zu prüfen.¹⁵ Die Verhältnismäßigkeit anhand der Bewertung einer solchen Kosten-Wirkungs-Relation, die auch personellen, technischen und wirtschaftlichen Aufwand, der dem Anbieter entsteht, einzubeziehen hat, erreicht ihre Grenze, wo die Anforderungen an die Sorgfaltspflichten so hoch werden, dass

ein dauerhafter Betrieb des Dienstes nicht oder nur noch unter erheblichen Schwierigkeiten umsetzbar ist.¹⁶ Zugrundeliegender Maßstab ist dabei ein „hohes Maß“, wobei alle implementierten Maßnahmen bei dieser Bewertung einzubeziehen sind. Mit dieser Formulierung geht zwar ein grundsätzlich ambitioniertes Verständnis einher, doch wird auch deutlich, dass nicht das höchste Maß erreicht werden muss, um Minderjährigen ein möglichst unbeeinträchtigtes Aufwachsen im digitalen Umfeld zu ermöglichen.¹⁷

III. Leitlinien der Kommission nach Art. 28 Abs. 4 DSA

Die Kommission kann nach Anhörung des Ausschusses Leitlinien herausgeben, um die Anbieter von Online-Plattformen bei der Anwendung von Art. 28 Abs. 1 DSA „zu unterstützen“. Entsprechend sind die Leitlinien grundsätzlich nicht rechtlich bindend, dennoch setzen sie Indizien und einen bedeutenden Maßstab auf den sich die Kommission bei der Anwendung von Art. 28 Abs. 1 DSA stützen wird, sodass ihnen im Rahmen behördlicher oder gerichtlicher Verfahren ein normenkonkretisierender Regelungscharakter zukommt. Zudem sind iRv durch die BzKJ beaufsichtigten Online-Plattformen mit Sitz in Deutschland die Leitlinienvorgaben vorrangig gegenüber dem Beispielkatalog des § 24a Abs. 2 JuSchG zu berücksichtigen.¹⁸ Die Umsetzung der Leitlinien begründet aber keine „automatische“ Konformität, da die Auslegung der Vorschrift letztlich dem EuGH vorbehalten ist. Ein Entwurf der Leitlinien ist im Mai 2025¹⁹ veröffentlicht und in die öffentliche Konsultation gegeben worden. Trotz ausstehender finaler Fassung lassen sich dem Entwurf bereits die grundlegenden Ansätze der künftigen Leitlinien mit hoher Wahrscheinlichkeit entnehmen.

Insbesondere äußern sich die Leitlinien zu allgemein zu berücksichtigenden Grundsätzen, die für alle Maßnahmen iSd Art. 28 Abs. 1 DSA gelten sollen.²⁰ Neben dem (1) Verhältnismäßigkeitsprinzip (s. unter ●●●) werden (2) die Berücksichtigung der Rechte des Kindes (darunter u.a. das Recht auf Schutz, Nichtdiskriminierung, Inklusion, Teilhabe, Privatsphäre, Information und freie Meinungsäußerung), (3) Privatsphäre, Sicherheit und Schutz „by design“ („höchste“ Standards während Konzeption, Entwicklung und dem Betrieb ihrer Dienste) und (4) altersgerechte Gestaltung (Entsprechung entwicklungsbezogener, kognitiver und emotionaler Bedürfnisse von Minderjährigen bei gleichzeitiger Gewährleistung ihrer Privatsphäre, Sicherheit und Schutz) erläutert. Anschließend werden die wichtigsten Maßnahmen aufgeführt, die Anbieter nach Ansicht der Kommission ergreifen sollten, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz zu gewährleisten. Dazu gehören die Risikobewertung, das Design der Dienste²¹, Melde- und Unterstützungssysteme für Nutzer und Tools für Erziehungsberechtigte²² sowie „Governance“²³. Dabei wird klargestellt, dass die beschriebenen Maßnahmen nicht erschöpfend sind. Möglich sind zB auch solche, die sich aus der Einhaltung anderer EU-Rechtsvorschriften oder der Befolgung nationaler Leitlinien zum Schutz Minderjähriger ergeben.²⁴ Innerhalb der einzelnen Abschnitte werden zT sehr konkrete Vorstellungen festgehalten.

Die Leitlinien ergänzen die Bestimmungen des DSA, insbesondere zu den Sorgfaltspflichten für VLOPs und VLOSEs (Very Large Online Search Engines) gem. Art. 33 ff. DSA, zu Melde- und Abhilfepflichten (Art. 16 ff. und 20 ff. DSA) oder Transparenzpflichten (Art. 14 f. und 24 DSA) und bauen auf bestehende Pflichten auf, ohne diese auszulegen oder zu ersetzen. Anbieter müssen daher eigenständig prüfen, ob zusätzliche Maßnahmen erforderlich sind. Art. 28 Abs. 1 DSA ist zudem im Kontext anderer unionsrechtlicher Vorgaben zum Schutz Minderjähriger

12 Vgl. Zeile 53 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU Kommission v. 13.5.2025, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>.

13 Mast/Kettemann/Dreyer/Schulz, Digital Services Act, 2024, Art. 28 Rn. 41.

14 Mast/Kettemann/Dreyer/Schulz, Digital Services Act, 2024, Art. 28 Rn. 45.

15 Vgl. Zeile 147 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

16 Mast/Kettemann/Dreyer/Schulz, Digital Services Act, Art. 28 DSA Rn. 56.

17 Vgl. ●●● Müller-Terpitz/Köhler/Holznapel, 2024, DSA Art. 28 Rn. 24.

18 Vgl. BeckOK JugendschutzR/Liesching, 4. Ed. 1.12.2024, DSA Art. 28 Rn. 56.

19 EU-Kommission, PM v. 13.5.2025, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>.

20 Alle Übersetzungen des Leitlinien Entwurfs sind durch den Autor vorgenommen worden.

21 Darunter: „6.1 Age assurance“; „6.1.1 Introduction and terminology“; „6.1.2 Determining whether to put in place age assurance measures“; „6.1.3 How to choose and implement age assurance measures“.

22 Darunter: „7.1 User reporting, feedback and complaints“; „7.2 User support measures“; „7.3 Tools for guardians“.

23 Darunter: „8.1 Internal processes and oversight“; „8.2 Training and awareness“; „8.3 Monitoring and evaluation“; „8.4 Transparency“.

24 Vgl. Zeile 138 f. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

im digitalen Raum zu verstehen. Die Leitlinien richten sich zwar primär an Minderjährige, können aber auch den Schutz aller Nutzer erhöhen.²⁵

1. Risikobewertung (Risk Review)

Für die Umsetzung des Art. 28 Abs. 1 DSA ist die Risikobewertung zentral. Grundlage ist eine strukturierte Analyse, die gemäß den Leitlinien mindestens folgende Punkte umfasst:²⁶

- Erstens ist die Wahrscheinlichkeit zu bewerten, mit der Minderjährige die Plattform nutzen.
- Zweitens sind die damit verbundenen Risiken anhand der „5Cs“-Typologie zu identifizieren, die sich nach deutschem Jugendschutzrecht in die Risikobereiche der Konfrontations- (content risks), der Interaktions- (contact und conduct risks) und der sonstigen Nutzungsrisiken (consumer und cross-cutting risks) einteilen lassen. Dabei können Aspekte wie Zweck, Design, Marketing, Funktionen, die Anzahl und Art der Nutzer sowie die tatsächlichen und erwarteten Verwendungszwecke relevant sein.
- Drittens sind bestehende und potenziell zusätzliche Maßnahmen zur Risikominimierung zu prüfen. Dabei ist stets zu bewerten, ob die Maßnahmen in einem angemessenen Verhältnis zur Risikominderung stehen. Aber auch mögliche negative Auswirkungen auf Kinderrechte, insbesondere in Bezug auf die Teilhabe am digitalen Umfeld, das Recht auf freie Meinungsäußerung und das Recht auf Information werden ausdrücklich genannt. Die Risikoüberprüfung sollte zudem im Lichte des Kindeswohls erfolgen und im Zuge wesentlicher Anpassungen des Dienstes der Online-Plattform stets aktualisiert werden, wobei eine Veröffentlichung der Ergebnisse empfohlen wird. Vorhandene Instrumente wie das „Child Rights Impact Assessment“²⁷ können iRd Risikobewertung unterstützend genutzt werden.

2. Altersprüfung (Age Assurance)

Einen zentralen Aspekt der Leitlinien bilden die Maßnahmen der Altersprüfung. Gemäß den Leitlinien werden unter „Age Assurance“ sämtliche Maßnahmen verstanden, mit denen der Zugang zu Online-Diensten altersabhängig reguliert wird, um Minderjährige vor ungeeigneten Online-Inhalten zu schützen.²⁸ Dabei werden drei Kategorien unterschieden: „Self-Declaration“, „Age Estimation“ und „Age Verification“. Die Selbstauskunft basiert auf freiwilligen Angaben der Nutzer und ist gemäß der Leitlinien nicht verlässlich genug, um den Anforderungen des Art. 28 Abs. 1 DSA Genüge zu tun. Age Estimation bietet eine Wahrscheinlichkeitsprognose über das Alter auf Grundlage technischer Verfahren (zB KI-gestützte Analyse), während die Age Verification auf verifizierte und sichere Identifikationsquellen (zB staatlicher Ausweis) zurückgreift und eine hohe Genauigkeit verspricht. IRe Verhältnismäßigkeitsprüfung ist zu ermitteln, ob für die vom jeweiligen Dienst ausgehenden Risiken eine Maßnahme der Altersprüfung erforderlich ist. Diesbezüglich „ist die Kommission der Ansicht, dass Anbieter auch die in anderen Abschnitten [der] Leitlinien dargelegten Maßnahmen als Alternative zu Maßnahmen zur Altersüberprüfung in Betracht ziehen sollten“²⁹.

Konkret ist eine Verifizierung (Age Verification) nach derzeitiger Auffassung der EU-Kommission in Konstellationen angezeigt, wenn

- EU- oder nationales Recht ein Mindestalter für den Zugang zu bestimmten Diensten oder Inhalten vorschreibt (zB Alkoholverkauf, Glücksspiel, Pornografie),
- Nutzungsbedingungen oder sonstige vertragliche Verpflichtungen eine Altersgrenze „ab 18 Jahren“ festlegen, um Minderjährige aufgrund identifizierter Risiken auszuschließen,

- andere Umstände vorliegen, in denen eine Risikobewertung des Anbieters ergibt, dass hohe Risiken für Minderjährige bestehen (einschließlich Kontakt- und Inhaltsrisiken), die nicht durch mildere Mittel beherrschbar sind.

Age Estimation wird dann als angemessen erachtet, wenn

- die Nutzungsbedingungen oder ähnliche vertragliche Verpflichtungen des Dienstes voraussetzen, dass ein Nutzer ein Mindestalter von unter 18 Jahren erreicht hat, um auf den Dienst zugreifen zu können und dabei die Bewertung des Anbieters angibt, ab wann die Online-Plattform für Minderjährige sicher genutzt werden kann,
- die Plattform nur „mittlere Risiken“ birgt und diese nicht durch weniger einschränkende Maßnahmen gemindert werden können.³⁰

Vor der Einführung einer dieser Methoden zur Altersüberprüfung, sollten Anbieter berücksichtigen, ob diese Methoden grob umschriebenen Maßstäben an Genauigkeit, Zuverlässigkeit, Umgehbarkeit, Datenschutzfreundlichkeit, -sparsamkeit und geringer Eingriffsintensität sowie der Nichtdiskriminierung entsprechen. Das künftige EU Digital Identity Wallet (EUid) soll einen entsprechenden Maßstab liefern.³¹ Zusätzlich sollen mindestens zwei verschiedene Methoden zur Altersverifizierung bzw. -schätzung sowie ein Beschwerdemechanismus im Falle fehlerhafter Altersfeststellung verfügbar sein, die wiederum den Vorgaben des Art. 20 DSA entsprechen sollen.³²

3. Tools für Erziehungs- und Sorgeberechtigte (Tools for Guardians)

„Tools for guardians“ finden ebenfalls Berücksichtigung iRd Leitlinien-Entwurfs. Darunter fallen digitale Funktionen oder Anwendungen, die Erziehungsberechtigten helfen, die Online-Aktivitäten, den Datenschutz und das Wohlbefinden ihrer Kinder zu steuern, zB durch Bildschirmzeitbegrenzung, Ausgabenbeschränkungen, oder das Verwalten von Kontoeinstellungen.³³ Die Kommission stellt klar, dass solche Tools nur ergänzend zu anderen Schutzmaßnahmen nach Art. 28 Abs. 1 DSA betrachtet werden sollten. Sie sollten weder alleinige Schutzmaßnahme zur Gewährleistung eines hohen Maßes an Privatsphäre, Sicherheit und Schutz noch sollten sie andere zu diesem Zweck getroffene Maßnahmen ersetzen. Es wird jedoch festgestellt, dass sie im Zusammenspiel mit anderen Maßnahmen zu einem solchen hohen Niveau beitragen können. Darüber hinaus wird näher bestimmt, welche Aspekte solche Tools im Einzelnen gewährleisten sollten.³⁴

4. Standardeinstellungen (Default settings)

Gemäß der Leitlinien spielen standardmäßige Voreinstellungen („Default Settings“) eine zentrale Rolle beim Schutz Minderjäh-

²⁵ Vgl. Zeile 87 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

²⁶ Vgl. Zeile 174 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

²⁷ Abrufbar unter: <https://www.nldigitalgovernment.nl/document/childrens-rights-impact-assessment-fill-in-document/>.

²⁸ Vgl. Zeile 210 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

²⁹ Vgl. Zeile 235 f. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³⁰ Vgl. Zeile 247 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³¹ Vgl. Zeile 268 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³² Vgl. Zeile 256 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³³ Vgl. Zeile 841 f. und 864 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³⁴ Vgl. Zeile 253 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

riger auf Online-Plattformen, da sie von den meisten jungen Nutzern nicht verändert werden und somit maßgeblich deren Nutzungserfahrung prägen. Die Kommission ist daher der Ansicht, dass Online-Plattformen, die für Minderjährige zugänglich sind und „Standardeinstellungen verwenden, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen auf ihren Diensten für die Zwecke des Artikels 28 Abs. 1 [DSA] ... zu gewährleisten“, näher bestimmte Anforderungen erfüllen sollten. Insbesondere wird betont, dass Kinder-Accounts von Beginn an auf das „höchstmögliche Schutzniveau“ ausgerichtet sein müssen. Zu den konkreten Anforderungen gehören zB restriktive Kommunikationsoptionen, die Deaktivierung sensibler Funktionen (zB Geolokalisierung oder Kamera) sowie Schutz vor exzessiver Nutzung (zB durch Abschaltung von Push-Nachrichten oder die Deaktivierung von Likes). Solche Voreinstellungen sollen u.a. regelmäßig überprüft werden, altersgerechte Erläuterungen enthalten und nicht dazu verleiten das Schutzniveau herabzusetzen.³⁵

5. Geschäftspraktiken (Commercial Practices)

Die Leitlinien betonen, dass Minderjährige besonders anfällig für die Wirkmechanismen kommerzieller Praktiken sind und daher eines besonderen Schutzes vor wirtschaftlicher Ausbeutung bedürfen. Trotz dieses Schutzbedarfs seien Minderjährige im digitalen Raum regelmäßig vielfältigen, dynamischen und personalisierten Werbestrategien ausgesetzt – etwa in Form von Werbung, Produktplatzierungen, In-App-Währungen, Influencer-Marketing oder KI-gestütztem „Nudging“.³⁶ Vor diesem Hintergrund und unbeschadet weiterer spezifischer Regelungen des DSA – insbesondere zu Werbung (Art. 26, 28 Abs. 2 DSA) und zur Vermeidung von „dark patterns“ (Art. 25 DSA) – empfiehlt die Kommission eine Reihe ergänzender Maßnahmen die vorgenommen werden sollten, um Art. 28 Abs. 1 DSA gerecht zu werden. Einige dieser Maßnahmen adressieren unmittelbar das Medium „Games“ bzw. können für Games von Relevanz sein. Die Leitlinien benennen zB die „Gewährleistung der Transparenz wirtschaftlicher Transaktionen in einer altersgerechten Weise und Vermeidung der Verwendung virtueller Zwischenwährungen wie Tokens oder Coins, die gegen echtes Geld eingetauscht und dann zum Kauf anderer virtueller Gegenstände verwendet werden können, was die Transparenz wirtschaftlicher Transaktionen verringern und für Minderjährige irreführend sein kann.“³⁷ Auch sei „sicher[zustellen], dass Minderjährige keinen Praktiken ausgesetzt sind, die zu übermäßigen oder unerwünschten Ausgaben oder Suchtverhalten führen können, indem ... gewährleiste[t wird], dass virtuelle Gegenstände wie Lootboxen, andere Produkte mit zufälligen oder unvorhersehbaren Ergebnissen oder Glücksspiel-ähnlichen Funktionen für Minderjährige nicht zugänglich sind, und indem ... eine Tren-

nung oder Friktion zwischen Inhalten und dem Kauf verwandter Produkte ein[ge]führ[t wird]“.³⁸ Daneben finden sich weitere Aspekte, zB dass Minderjährige „keinen manipulativen Design-Techniken wie Knappheit, intermittierenden oder zufälligen Belohnungen ausgesetzt sind“ oder „sicher[zustellen] ist, dass Minderjährige keinen unerwünschten Käufen ausgesetzt sind, zB durch den Einsatz wirksamer Tools für Erziehungsberechtigte.“ Auch die Kennzeichnung werblicher Inhalte oder die direkte Ansprache von Minderjährigen iRv Werbung werden genannt.

6. Selbstregulierung – Orientierungsfunktion und Vollzugshilfe

Das auf nationaler Ebene in Deutschland bewährte Prinzip der regulierten Selbstregulierung findet sich in dieser Form zwar nicht unmittelbar in den Leitkriterien wieder, allerdings finden sich an verschiedenen Stellen Anknüpfungspunkte iRd Leitlinien-Entwurfes, die typische Aufgabenbereiche von Selbstkontrolleinrichtungen aufgreifen.³⁹ So gewinnen Empfehlungen und Positionen von Selbstregulierungseinrichtungen wie der USK als One-Stop-Shop der Games-Branche⁴⁰ im Bereich des Jugendmedienschutzes grundsätzlich an rechtlicher und praktischer Relevanz.⁴¹ Sie unterstützen ihre Mitglieder dabei, Schutzpflichten in Bezug auf Minderjährige rechtskonform und wirksam in die Praxis umzusetzen. Mit ihrer Expertise tragen sie zur Ausformung anerkannter Mindeststandards bei. Damit bieten sie Anbietern Orientierung, schaffen faktische Erwartungshorizonte und fördern zugleich Kohärenz und Transparenz im Vollzug. Diese Rolle entspricht auch dem internationalen Verständnis eines kooperativen, multi-stakeholder-basierten Jugendmedienschutzes, wie er u.a. von den Vereinten Nationen gefordert wird.⁴² Vor diesem Hintergrund erscheint die Zusammenarbeit mit anerkannten Selbstkontrolleinrichtungen wie zB USK sinnvoll sowie ein sachgerechtes und verantwortungsvolles Mittel zur Erfüllung regulatorischer Anforderungen unter dem DSA.

7. Ungenutzte Potenziale und Inkonsistenz

Der Leitlinien-Entwurf der Kommission bietet zwar einen wichtigen Orientierungsrahmen für Online-Plattformen, bleibt jedoch in Bezug auf Kohärenz, Praktikabilität und Systematik hinter den Erwartungen zurück. Trotz ihres gem. Art. 28 Abs. 4 DSA empfehlenden Unterstützungscharakters, vermittelt die Vielzahl an Anforderungen und „Soll“-Formulierungen teils den Eindruck einer faktischen Verpflichtung zur kumulativen Umsetzung der genannten Aspekte, was im Widerspruch zum zentralen Verhältnismäßigkeitsprinzip steht. Eine beispielhafte Darstellung wie in § 24a Abs. 2 JuSchG wäre zugunsten der Rechtsklarheit zu bevorzugen. Zudem erschweren widersprüchliche Aussagen eine konsistente Anwendung, etwa wenn „höchste Standards“ verlangt werden, obwohl Art. 28 Abs. 1 DSA nur ein „hohes Maß“ vorschreibt. Der wiederholt umschriebene Maßstab mit Begriffen wie „easy to use“, „intuitive“ oder „engaging“ können zudem dazu führen, dass selbst engagierte Anbieter dem Vorwurf der Benutzerunfreundlichkeit ausgesetzt sind. Die Leitlinien liefern kaum Hinweise zur nutzerzentrierten Umsetzung oder Priorisierung, sodass bereits die schiere Anzahl an Maßnahmen als unpraktikabel kritisiert werden könnte.

Bei zentralen Begriffen fehlt es zudem an Klarheit, zB bleiben „mittlere Risiken“ ohne Definition, was kaum Orientierung bietet. Auch kommt es im Bereich der Risikobestimmungen zu einer unangemessenen Vermischung jugendschutz- und Verbraucherschutzrechtlicher Maßstäbe, etwa wenn Volljährigkeit laut AGBs als Auslöser für AVS-pflichten dient. Hier sollte eine klare Trennung beider Rechtsbereiche gemäß ihrem jeweiligen

³⁵ Vgl. Zeile 383 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³⁶ Vgl. Zeile 612 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³⁷ Vgl. Zeile 653 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³⁸ Vgl. Zeile 661 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

³⁹ Vgl. insb. Zeilen 908 ff. („Governance“) und 953 ff. („Monitoring and evaluation“), aber auch Zeilen 635 ff. und 714 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.

⁴⁰ Hentsch/von Petersdorff MMR-Beil. 8/2020, 3 ff.

⁴¹ Vgl. ●● Müller-Terpitz/Köhler/Holznapel, 2024, DSA Art. 28 Rn. 21–23; ebenso Mast/Kettemann/Dreyer/Schulz, 2024, DSA Art. 28 Rn. 71 f., der iRd Zieldimension „Schutz“ u.a. Prozesse und Verfahren hervorhebt und dabei die Zusammenarbeit mit externen Experten im Kinder- und Jugendmedienschutz, die Einrichtung eines Kinder- und Jugendschutzbeauftragten (über § 7 JMStV hinaus) oder die Kooperation mit externen Beratungs- und/oder Beschwerdestellen benennt.

⁴² Vgl. UN-Kinderrechtsausschuss, Allg. Bemerkung Nr. 25 (2021), Abschnitt V, „C. Coordination“, Nr. 27.

Schutzzweck bestehen bleiben, um das Risiko divergierender Rechtsentwicklungen aufgrund von Doppelregulierungen nicht weiter zu vertiefen.

Verschenktes Potenzial zeigt sich in der mangelnden Berücksichtigung nachweislich wirksamer Modelle an präventiven, selbstregulatorischen Ansätzen. Als Beispiel dient insbesondere das automatisierte Bewertungssystem der International Age Rating Coalition (IARC), das aus einer globalen Kooperation eben solcher Institutionen heraus entstanden und mittlerweile in Deutschland staatlich geprüft und anerkannt worden ist.⁴³ IARC erteilt auch Alterskennzeichen im Bereich nutzergenerierter Spiele (zB Fortnite). Alterskennzeichen, die Nutzungsrisiken und Vorsorgemaßnahmen iRd Altersbewertung berücksichtigen und entsprechende Zusatzhinweise zu enthaltenen Funktionalitäten sowie den wesentlichen Gründen der Alterskennzeichnung vergeben, heben das Schutzniveau erheblich und tragen auch zur geforderten Transparenz bei (vgl. 8.4 des Leitlinien-Entwurfs). Dies geschieht schon allein aufgrund ihrer sensibilisierenden Wirkung und umso mehr in Kombination mit technischen Filtern wie Parental Controls. Für den Raum Deutschland erfolgt dies auf Basis des JuSchG und künftig auch des JMStV durch die USK.

Besonders schwer wiegen Aussagen im Hinblick auf technische Altersprüfungen und Tools for Guardians, wie Parental Controls. Systematisch bleibt der Fokus somit übermäßig stark auf AVS und Age Estimation gerichtet. So knüpfen etwa viele Maßnahmen des Entwurfs an die Kenntnis über das Alter des Nutzers. Vor allem aber sollen formal zwar alternativen zur Altersprüfung möglich sein (s. unter ●●●), der naheliegendsten Alternative (Parental Controls) wird jedoch ihre alleinige Schutzwirkung nahezu abgesprochen, obwohl sie mit hohem Schutzpotenzial zentrale Aspekte wie Teilhabe und das Elternprivilegs (Art. 6 GG) wahren und die Grundlage für viele weitere Maßnahmen bilden. Ohne solche Tools lassen sich Schutzmaßnahmen kaum alters- und situationsgerecht ausgestalten. Besonders deutlich wird dies anhand der Empfehlungen zu „default settings“, deren Wirkung sich erst durch Parental Controls entfaltet. Diese scheinbare Entwertung ist besonders fragwürdig, da dem Bereich der „default settings“ dem Wortlaut der Leitkriterien nach besonderes Gewicht beigemessen wird („providers ... that use default settings to ensure a high level of privacy, safety, and security of minors on their service“) und damit scheinbar eine Alternative zur Altersprüfung darstellen sollen, obwohl sie mit Tools for Guardians sachlich unmittelbar miteinander verbunden sind. Neben dem Fokus auf AVS auch für den Bereich der Volljährigkeit wird jedoch die für den Anwendungsbereich des Art. 28 Abs. 1 DSA zentrale Diskrepanz zu dem Merkmal „für Minderjährige zugänglich“ nicht nachvollziehbar aufgelöst. Darüber hinaus offenbart eine Analyse der relevanten Risikokategorien, dass verpflichtende Altersüberprüfungen im vorliegenden Kontext auch hinsichtlich ihrer Effektivität und Verhältnismäßigkeit fragwürdig sind, um die zentrale Schutzziele im digitalen Raum zu erreichen. So hängen verhaltensbezogene Risiken weniger vom „biologischen“ Alter eines Nutzers ab als vielmehr von sozialen Interaktionen sowie den strukturellen Ge-

benheiten der Plattformen. Die bloße Kenntnis des Alters beeinflusst hingegen nicht das konkrete Verhalten Minderjähriger. AVS verhindern weder, dass junge Nutzer persönliche Informationen preisgeben, noch dass sie sich riskant oder exzessiv im digitalen Raum bewegen. Anzumerken ist außerdem, dass die Erfahrungswerte nach deutschem Jugendschutzrecht im Hinblick auf einheitliche EU-Standards über das „Digital Identity Wallet“ belegen, dass ein solcher Ansatz in der Praxis schwer umsetzbar sein dürfte.

IV. Fazit

Der Leitlinien-Entwurf enthält zahlreiche gute Ansätze und Konkretisierungen, bleibt aber in seiner Struktur, Kohärenz und praktischen Umsetzbarkeit hinter dem Anspruch eines stringenten und realitätsnahen Regelungskonzepts zurück. Für die wirksame Umsetzung des Art. 28 Abs. 1 DSA ist eine weitergehende Präzisierung, Priorisierung und Verzahnung mit bestehenden Instrumenten – auch auf nationaler Ebene – erforderlich. Gerade im Hinblick auf die Altersprüfungen bleibt die Systematik bzw. das Ineinandergreifen der Maßnahmen und das Ziel der Leitlinien insgesamt nicht eindeutig. Es bleibt allein die Vermutung, dass Altersprüfungen künftig eine „Weichenstellung“ hinsichtlich der Zugänglichkeit der jeweiligen Funktionen und Inhalte auf Online-Plattformen darstellen sollen. In Anbetracht des Anwendungskriteriums der „für Minderjährige zugänglichen“ Online-Plattform, können solche Systeme aber wohl nicht zur Festsetzung pauschaler Zugangshürden iSe geschlossenen Benutzergruppe nach JMStV gewollt sein.

Schnell gelesen ...

- Art. 28 DSA etabliert erstmals verbindliche Schutzstandards für Minderjährige auf Online-Plattformen.
- Der Leitlinien-Entwurf der EU-Kommission bleibt in Systematik, Kohärenz und Umsetzbarkeit hinter den Erwartungen zurück.
- Die starke Fokussierung auf technische Altersverifikation verschenkt Potenzial im Hinblick auf verhältnismäßige und bewährte (selbstregulatorische) Ansätze wie Parental Controls und Alterskennzeichen.
- Unklare Begriffe und widersprüchliche Maßstäbe erschweren die rechtskonforme Anwendung durch Plattformanbieter.



Lorenzo von Petersdorff

ist stellvertretender Geschäftsführer und Legal Counsel der Unterhaltungssoftware Selbstkontrolle (USK), Leiter des Geschäftsbereichs USK.online sowie stellvertretendes Mitglied im Beirat der Stiftung Digitale Spielekultur.

⁴³ Vgl. PM der USK v. 25.4.2025, abrufbar unter: <https://usk.de/starker-digitaler-kinder-und-jugendschutz-automatisiertes-system-der-usk-fuer-alterskennzeichen-auf-online-spieleplattformen-ueberzeugt-jugendschutzbehoerden-der-bundeslaender/>.

Inhaltsmoderation in Online-Spielen nach dem DSA

Erste Erfahrungen mit Mehrspielermodus zur Umsetzung der Transparenzpflichten aus Art. 14 bis 17 DSA

Melde- und Abhilfeverfahren

Der Digital Services Act (DSA) erweitert die Regulierung von Online-Spielen, indem er neue Transparenzpflichten für die Inhaltsmoderation vorschreibt. Obwohl es unter Anbietern von Online-Spielen seit jeher abgestufte Systeme zur Moderation gab, werden diese nun einheitlicher und strenger reglementiert. Anbieter müssen die Beschränkungen für nutzergenerierte Inhalte noch einfacher, klarer und verständlicher fassen, vor allem gegenüber minderjährigen Spielern. Auch müssen sie jährliche Transparenzberichte über die Meldungen und Abhilfemaßnahmen betreffend die Inhalte veröffentlichen. Zuletzt

müssen Abhilfeentscheidungen nun noch ausführlicher begründet und dezidierte Beschwerdeverfahren vorgehalten werden. Der vorliegende Beitrag beleuchtet, wie die gut gemeinten Regelungen derzeit in der Praxis vor allem für eins sorgen: Mehr organisatorischen Aufwand für die Anbieter ohne klare Verbesserungen für die Nutzer. Beleuchtet werden insbesondere die Herausforderungen bei der Formulierung der Beschränkungen für Inhalte, der Erstellung der Transparenzberichte und der Änderungen in den Abhilfe- und Beschwerdeverfahren.

Lesedauer: ●● Minuten

I. Einleitung

Mit dem Inkrafttreten des Digital Services Act (DSA) vollzieht sich ein bedeutender Wandel in der Regulierungslandschaft für Online-Spiele mit Mehrspielermodus. Anbieter solcher Spiele werden zumeist als Hosting-Dienste eingeordnet, da dort Spieler eigene Inhalte wie Sprach- und Text-Chat sowie Bilder, Screenshots, Videos etc mit anderen Spielern teilen können. Dies Teil von Inhalten ist eine Nebenfunktion des gemeinsamen Spielens. Es dient vor allem zur Koordination bei der Bewältigung gemeinsamer Aufgaben im Spiel selbst. Es erstreckt sich aber zuweilen auch auf den geselligen Austausch außerhalb des Spiels in zugehörigen Chaträumen, Foren, Instant-Messengern etc, sofern sie vom Spieleanbieter ergänzend zum Spiel bereitgestellt werden. Sowohl innerhalb als auch außerhalb des Spiels fallen große Mengen an nutzergenerierten Inhalten an. Für den Umgang mit solchen Inhalten gibt es seit jeher bei Spieleanbietern abgestufte Sanktionssysteme, der DSA hebt diese nun aber auf eine ganz neue Stufe.

Seit dem Inkrafttreten des DSA müssen Spieleanbieter nämlich insbesondere neue Transparenzpflichten bei der Inhaltsmoderation aus Art. 14 bis 17 DSA erfüllen. Unter Inhaltsmoderation versteht man die Verfahren und organisierten Praktiken zur Überprüfung von nutzergenerierten Inhalten, die auf Hosting-Diensten veröffentlicht werden, um festzustellen, ob ein Inhalt den eigenen AGB und dem öffentlich-rechtlichen Rechtsrahmen entspricht.¹ Der Rechtsrahmen besteht in Deutschland vor allem aus dem DSA, der EU-Verordnung zur Bekämpfung terroristischer Online-Inhalte, dem Strafgesetzbuch, dem Jugendschutzgesetz und dem Jugendmedien-schutz-Staatsvertrag. Spieleanbieter beschäftigen Moderatoren, die in ihrem Auftrag oder als Stellvertreter die Inhaltsmoderation vornehmen. Spieleanbieter haben ein Interesse an einer wirksamen Inhaltsmoderation, da sie die Attraktivität des Spielangebots erhöht und das Haftungsrisiko wegen Rechtsverstößen verringert. Dieser Beitrag beschreibt erste Erfahrungen bei der Umsetzung der Transparenzpflichten aus Art. 14 bis 17 DSA durch Spieleanbieter.

¹ BNetzA, Staus-quo spezifischer Maßnahmen von Hostingdiensten zur Inhaltsmoderation, 2024, abrufbar unter: <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Internet/TerrorOnlin/Studie.pdf>.

II. Beschränkungen für nutzergenerierte Inhalte in den AGB

Für die Spieleanbieter nehmen AGB eine wichtige Rolle ein. Die AGB setzen nämlich einerseits den vertraglichen Rechtsrahmen zwischen dem Nutzer des Spiels und dem Spieleanbieter. Sie haben aber auch eine wichtige faktische Ordnungswirkung zwischen den Nutzern. Da die Nutzer in Online-Spielen mit Mehrspielermodus interagieren, ist es für sie von entscheidender Bedeutung, dass sich auch ihre Mitspieler an die vom Spieleanbieter vorgegebenen Regeln halten. Schließlich existieren mangels Vertragsbeziehungen keine unmittelbaren Ansprüche zwischen den Nutzern. Die Nutzer beschwerten sich daher häufig beim Spieleanbieter über Verstöße anderer Nutzer.

Die Darlegung von Regeln für nutzergenerierte Inhalte hat einen hohen Stellenwert, weil dadurch die Atmosphäre der Kommunikation zwischen den Nutzern stark beeinflusst wird. Dies hat Auswirkungen auf das „Miteinander“ der Nutzer eines Spiels, dessen Faszination insbesondere vom Mehrspielermodus lebt. Das Maß der Regulierung durch den Spieleanbieter ist für einige Spieler ein wichtiger Faktor für die Auswahl der von ihnen genutzten Spiele. Einige Spieler schätzen es etwa, wenn es in Foren nicht erlaubt ist, andere Spieler in einer Weise anzugehen, die zwar unhöflich ist, aber deutlich unter einer etwaigen Strafbarkeitsschwelle liegt. So wird es zB unterschiedlich gehandhabt, ob man einen anderen Nutzer als „Noob“ bezeichnen darf. „Noob“ ist kein Schimpfwort iES, sondern eine Bezeichnung für einen unerfahrenen Spieler. Der Begriff ist gleichwohl leicht abschätzig gemeint. Der Begriff leitet sich vom englischen Wort „newbie“ ab, was so viel wie „Anfänger“ bedeutet. Ein Noob zeichnet sich durch seine mangelnde Erfahrung aus, die sich darin äußert, dass er ungeschickte Spielzüge macht.

Art. 14 Abs. 1 S. 1 DSA legt fest, dass die Spieleanbieter neben den Beschränkungen für nutzergenerierte Inhalte auch Angaben machen „zu allen Leitlinien, Verfahren, Maßnahmen und Werkzeugen, die zur Moderation von Inhalten eingesetzt werden, einschließlich der algorithmischen Entscheidungsfindung und der menschlichen Überprüfung, sowie zu den Verfahrensregeln für ihr internes Beschwerdemanagementsystem.“ Der Sinn dieser Regelung liegt darin, dass dem Nutzer schon bei Ab-

schluss seines Vertrags mit dem Spieleanbieter vor Augen geführt werden soll, welche Regeln gelten, wenn der Spieleanbieter prüft, ob nutzergenerierte Inhalte den Regeln entsprechen, die in den AGB ausgestellt wurden. Der Begriff der „Moderation von Inhalten“ ist in Art. 3 lit. t DSA wortreich definiert. Es handelt sich danach um „die – automatisierten oder nicht automatisierten – Tätigkeiten der Anbieter von Vermittlungsdiensten, mit denen insbesondere rechtswidrige Inhalte oder Informationen, die von Nutzern bereitgestellt werden und mit den allgemeinen Geschäftsbedingungen des Anbieters unvereinbar sind, erkannt, festgestellt und bekämpft werden sollen, darunter auch Maßnahmen in Bezug auf die Verfügbarkeit, Anzeige und Zugänglichkeit der rechtswidrigen Inhalte oder Informationen, zB Herabstufung, Demonetisierung, Sperrung des Zugangs oder Entfernung, oder in Bezug auf die Fähigkeit der Nutzer, solche Informationen bereitzustellen, zB Schließung oder Aussetzung des Kontos eines Nutzers“.

Typischerweise setzen Anbieter von Spielen mit Mehrspielermodus schon seit vielen Jahren – also lange vor Inkrafttreten des DSA – auf ein abgestuftes Sanktionssystem. Die Ausgestaltung dieses Systems ist zwar je nach Spieleanbieter individuell, es haben sich aber über die Zeit Ähnlichkeiten herausgebildet. Die niedrigste Eingriffsschwelle stellt die Entfernung von Inhalten dar, da dann nur die Inhalte der Nutzer nicht mehr aufrufbar sind, die Nutzer selbst aber keinen Maßnahmen ausgesetzt sind, die sie in der Zukunft einschränken. Die nächste Stufe der Eskalation besteht darin, die Nutzungsmöglichkeiten des Spielers einzuschränken, etwa durch das Abschalten der Chatfunktion, Entzug der Berechtigung der Veröffentlichung von Forenbeiträgen sowie Deaktivierung der Voice-Chat-Funktion (sofern das Spiel eine solche Funktion bereithält). Diese Maßnahmen sollen sicherstellen, dass es zukünftig nicht mehr zu Verletzungen kommt, ohne dem Nutzer aber die Möglichkeit zu nehmen, das Spiel zu spielen. Die dritte Eskalationsstufe besteht in der vorübergehenden, aber vollständigen Sperrung des Zugangs zum Spiel. Ein solches vorübergehendes Einfrieren des Zugangs bezeichnet man in der Games-Branche als „Suspension“. Die Spieler haben also für eine bestimmte Zeit keine Möglichkeit, das Spiel zu benutzen. Nach dieser Zeit wird dem Spieler der Zugang aber wieder eingeräumt. Die höchste Eskalationsstufe besteht in der dauerhaften Sperrung des Zugangs zum Spiel (in der Games-Branche als „Ban“ bezeichnet).

Art. 14 Abs. 1 S. 2 DSA regelt, dass die Angaben nach Art. 14 Abs. 1 S. 1 DSA in klarer, einfacher, verständlicher, benutzerfreundlicher und eindeutiger Sprache abgefasst und in leicht zugänglicher und maschinenlesbarer Form öffentlich zur Verfügung gestellt werden müssen. Die Spieler sollen also die Möglichkeit haben, die Regeln und Verfahren des Spieleanbieters zur Moderation von Inhalten leicht nachzuvollziehen. Die Spieleanbieter stehen hier vor der Herausforderung, die Regeln hinreichend konkret dazustellen, weil starke Abstraktionen schwieriger zu verstehen sind. Es ist allerdings zu beachten, dass eine zu konkrete Festlegung die Gefahr birgt, dass man bestimmte Fälle nicht vorausgesehen hat, die ungeregelt geblieben sind. Spieleherstellern ist daher zu raten, Listen mit Beispielen von nicht tolerierten Inhalten in die Nutzungsbedingungen aufzunehmen und diese Listen regelmäßig zu ergänzen, wenn Verhaltensweisen auftreten, die man nicht erfasst hatte, aber zukünftig sanktionieren will.

Typische nicht akzeptierte und in AGB untersagte Verhaltensweisen sind Verletzungen der Persönlichkeit, Verstöße gegen das Urheberrecht oder die Verbreitung von pornografischen, Gewalt verherrlichenden, sexistischen, rechts- oder linksextremen Inhalten.

III. Kommunikation der Beschränkungen gegenüber minderjährigen Spielern

Neben den im DSA genannten allgemeinen Beschränkungen für Vermittlungsdienste werden im Digital Services Act (DSA) auch ausdrückliche Regelungen genannt, die den Schutz von Kindern und Jugendlichen sicherstellen sollen.² Der Wille des EU-Gesetzgebers, Minderjährige im Online-Umfeld stärker zu schützen, äußert sich u.a. in Art. 14 Abs. 3 DSA.³ Danach bestehen für Anbieter von Vermittlungsdiensten, die sich „in erster Linie“ an Minderjährige richten oder überwiegend von solchen genutzt werden, besondere Verpflichtungen zu der Verständlichkeit der Nutzungsbedingungen.

1. Adressatenkreis: „In erster Linie“ an Minderjährige

Der DSA lässt offen, ab welcher Schwelle eine überwiegende Nutzung von Minderjährigen vorliegt.⁴ Ausschlaggebend ist entweder die objektive Ausrichtung des Vermittlungsdienstes oder die Anzahl der minderjährigen Nutzer.⁵ Die Ausrichtung lässt sich zB an Gestaltung oder Vermarktung des Dienstes ableiten. Für die Annahme einer überwiegenden Nutzung durch Minderjährige ist eine einfache Mehrheit von über 50% ausreichend.⁶

Viele Spiele erwecken aufgrund ihrer bunten Grafik den Eindruck, dass sie hauptsächlich von Kindern gespielt werden, während die tatsächliche Nutzerbasis oft Personen sind, die über 30 Jahre alt sind und manchmal sogar deutlich älter. Es kommt hier also auf den Einzelfall an, der genau betrachtet werden muss.

In der Games-Branche schließen die meisten Anbieter von Mehrspieler-Online-Spielen in den AGB Nutzer unter 16 Jahren (teilweise sogar Nutzer unter 18 Jahren) aus.

2. Anforderungen an die Formulierung

Sind Minderjährige, also Personen unter 16 Jahren zugelassen, muss eine Aufbereitung der AGB in verständlicher Form erfolgen, um in jedem Fall die Möglichkeit der Kenntnisnahme zu gewährleisten.⁷ Der DSA lässt offen, wie genau die Anforderungen an eine jugendgerechte Formulierung aussehen sollten.⁸

Die Texte müssen so formuliert sein, dass Minderjährige sie verstehen können, mithin kind- und jugendgerecht. Eine ähnliche Formulierung findet sich in § 24a Abs. 2 S. 8 JuSchG, wonach „die für die Nutzung wesentlichen Bestimmungen der Allgemeinen Geschäftsbedingungen in kindgerechter Weise“ darzustellen sind. Allerdings ändert auch eine verständlichere Version der Nutzungsbedingungen nichts an der Vermutung, dass Kinder und Jugendliche auch diese AGB in den meisten Fällen nicht lesen würden.⁹

3. Anforderungen an den Inhalt

„Doppelte AGB“, also spezielle „Jugend-AGB“ neben den herkömmlichen Geschäftsbedingungen zu etablieren würde die Minderjährigen jedoch ungebührlich benachteiligen.¹⁰ Folglich sind „jugendgerechte AGB“ iSd Art. 14 Abs. 3 DSA gerade keine AGB, sondern lediglich erklärende Angaben, die neben den

2 BzKJAKTUELL 1/2024, 8, (11).

3 Erwägungsgrund 46 DSA; Müller-Terpitz/Köhler, DSA/Barudi, ●●● Auflage oder Jahr ergänzen ●●● Art. 14 Rn. 22.

4 Müller-Terpitz/Köhler, DSA/Barudi, ●●● Art. 14 Rn. 22.

5 Erwägungsgrund 46 DSA.

6 Hofman/Raue, DSA, ●●● Art. 14 Rn. 70.

7 Müller-Terpitz/Köhler, DSA/Barudi, ●●● Art. 14 Rn. 22.

8 Müller-Terpitz/Köhler, DSA/Barudi, ●●● Art. 14 Rn. 22.

9 Dregelies MMR 2022, 1033 (1036).

10 Liesching, ●●● Titel, Auflage/Jahr ergänzen ●●●, § 24a Rn. 67.

geltenden Geschäftsbedingungen stehen.¹¹ Dafür spricht auch der Wortlaut des Art. 14 Abs. 3 DSA, in dem von einer Erläuterung der Bestimmungen und nicht zB einer Abfassung gesonderter AGB die Rede ist.¹²

Durch die Formulierung in Art. 14 Abs. 3 DSA, wonach „Bedingungen und jegliche Einschränkungen für die Nutzung des Dienstes“ erläutert werden müssen, ist der Vermittlungsdienst dazu verpflichtet, die gesamten AGB jugendgerecht aufzubereiten und zur Verfügung zu stellen.¹³ Damit ist der DSA an dieser Stelle genauer als das JuSchG, das in § 24a lediglich eine Aufbereitung der „wesentlichen Bestimmungen“ fordert. Besonders sollten dabei jene Vorschriften der AGB deutlich transponiert werden, die sich mit den Hauptleistungspflichten sowie der Verarbeitung der personenbezogenen Daten befassen.¹⁴

Nach dem Wortlaut des Art. 14 Abs. 3 DSA müssen auch in die AGB einbezogene Regeln wie Community Richtlinien jugendgerecht aufbereitet werden, insofern von „Bedingungen und jeglichen Einschränkungen“ die Rede ist.¹⁵ Die konkreten Anforderungen an die Erläuterungen in jugendgerechter Sprache sind vom Gesetzgeber allerdings nicht festgelegt worden und bieten mithin einen relativ weiten Gestaltungsspielraum.¹⁶ So könnten sich Anbieter zB audiovisueller Darstellungen der zu erläuternden Inhalte, Erklärvideos, Piktogrammen oÄ bedienen.¹⁷ Dies könnte auch die o.g. Problematik lösen, dass Texte eventuell von Kindern und Jugendlichen nicht gelesen werden könnten. Darüber hinaus sollten die Erläuterungen auch in den verschiedenen Muttersprachen der Nutzergruppen verfügbar sein.¹⁸

4. Kommunikation mit Minderjährigen

In Bezug auf die Datenverarbeitung durch Games-Anbieter können nach Art. 8 Abs. 1 S. 1 DS-GVO Minderjährige ab 16 Jahren selbst in die Datenverarbeitung einwilligen, sofern dies ausdrücklich und freiwillig geschieht und die minderjährige Person

über die konkrete Datenverarbeitung und ihre Rechte hinreichend (mithin auch jugendgerecht) informiert worden ist. Jüngere Nutzer von Games müssten zu der Einwilligung in die Datenverarbeitung entweder eine Zustimmung der gesetzlichen Vertreter zu ihrer eigenen Einwilligung oder eine direkte Einwilligung der Sorgeberechtigten vorweisen. Eine Abfrage und Überprüfung des Alters kann iRe sog. Parental Control Systems erfolgen, um dem Jugendschutz und Art. 8 Abs. 2 DS-GVO gerecht zu werden, falls der Minderjährige unter 16 Jahre alt ist.¹⁹ Große Spieleanbieter wie Epic, Nintendo oder Roblox haben dafür ausgefeilte Systeme.

IV. Transparenzberichtspflichten

1. Neue Vorgaben und Stand der Umsetzung

Eine neue Herausforderung für Anbieter von Online-Spielen stellen die gem. Art. 15 DSA zu erstellenden jährlichen Transparenzberichte dar. Es ist zu beobachten, dass solche Berichte bislang nur von wenigen großen Anbietern veröffentlicht wurden.²⁰ Dagegen finden sich bisher kaum Berichte von mittelständischen Anbietern,²¹ obwohl diese als Hostingdiensteanbieter mehrheitlich von Art. 15 DSA erfasst sein dürften. Auch wenn Klein- und Kleinstunternehmen mit weniger als 50 Mitarbeitern und weniger als 10 Mio. EUR Jahresumsatz gem. Art. 15 Abs. 2 DSA von der Berichtspflicht ausgenommen sind, dürften schätzungsweise 30-40 Spieleanbieter mit Sitz in Deutschland gleichwohl weiter der Berichtspflicht unterliegen.²² Dass es bisher kaum Transparenzberichte aus dem Mittelstand gibt, mag daran liegen, dass es zum einen ein Informationsdefizit über das Bestehen der Rechtspflicht gibt, zum anderen der Aufwand der Erstellung der Berichte sehr hoch ist. Als Beispiel sei hier angeführt, dass bei der InnoGames GmbH als mittelständischem Anbieter für die Erstellung des Transparenzberichtes 2024 ca. 100 Personenstunden anfielen.

2. Form der Berichte

Die für das erste Berichtsjahr 2024 von Spieleanbietern veröffentlichten Transparenzberichte unterschieden sich in der Form noch auffällig: Einige Anbieter veröffentlichten aufwändig gestaltete Berichte mit wortreichen Erläuterungen, andere schlichte Zettel mit mehr oder weniger unkommentierten Tabellen.²³ Bei einigen Anbietern waren die Berichte zwei DIN A4-Seiten lang, bei anderen 38 DIN A4-Seiten – und das sogar bei vergleichbar großen Anbietern.²⁴ Ab dem Berichtsjahr 2025 will die EU-Kommission diesen „Wildwuchs“ nun mit einer Durchführungsverordnung gem. Art. 15 Abs. 3 DSA beenden.²⁵ Ab Juli 2025 müssen alle Anbieter einheitliche Meldebögen verwenden. Spieleanbieter betrifft dies – anders als die halbjährlich berichtspflichtigen sehr großen Online-Plattformen (Very Large Online Platforms – VLOPs) und -Suchmaschinen (Very Large Online Search Engines – VLOSEs) – dann erstmals zum Abgabetermin für das Kalenderjahr 2025 am 28.2.2026. Die Meldebögen sind als CSV- und XLSX-Tabellenvorlagen auf der Kommissions-Webseite abrufbar und werden von einem 32 Seiten langen Ausfüllhinweis begleitet.²⁶

3. Kritik an Formvorgaben

Bei allem nachvollziehbaren Bemühen um Einheitlichkeit und Vergleichbarkeit ist der neue Meldebogen ein bürokratischer Alptraum: Es gibt nur eine Vorlage für alle Anbieterarten, egal ob es sich um einen einfachen Vermittlungsdienst oder eine sehr große Online-Plattform oder -Suchmaschine handelt. Folglich besteht jeder Bogen aus 11 Tabellenblättern, von denen die größten 180 Zeilen lang und 20 Spalten breit sind. Spieleanbieter müssen also zunächst all diejenigen Zellen herauslöschen, die für sie gar nicht anwendbar sind. Dann müssen sie in den unhandlichen Tabellenvorlagen seitenweise Zahlen eintragen. Zu

¹¹ Hofmann/Raue, DSA, ●●● Art. 14 Rn. 71.

¹² Hofmann/Raue, DSA, ●●● Art. 14 Rn. 71

¹³ FSM, Jugendgerechte AGB – Die rechtliche Interpretation des Art. 14 Abs. 3 DSA, S. 2, abrufbar unter: https://www.jff.de/fileadmin/user_upload/jff/projekte/ugendgerechte_AGB/Jugend-AGB_Rechtliche_Interpretation_DSA.pdf.

¹⁴ Erdemir/Berzen/Dreyer, JuSchG, ●●● § 5 Rn. 89.

¹⁵ FSM, Jugendgerechte AGB – Die rechtliche Interpretation des Art. 14 Abs. 3 DSA, S. 2, abrufbar unter: https://www.jff.de/fileadmin/user_upload/jff/projekte/ugendgerechte_AGB/Jugend-AGB_Rechtliche_Interpretation_DSA.pdf.

¹⁶ BzKJAKTUELL 1/2024, 24 (25).

¹⁷ Liesching, ●●● § 24a Rn. 66.

¹⁸ Erdemir/Berzen/Dreyer, JuSchG, ●●● § 5 Rn. 91.

¹⁹ Bäsch/Hentsch MMR-Beil. 8/2021, 3 (6).

²⁰ Electronic Arts, abrufbar unter: <https://media.contentapi.ea.com/content/dam/eacom/common/transparency-report-2024.pdf>; Nintendo abrufbar unter: https://www.nintendo.com/eu/media/downloads/legal_1/DSA_Transparency_Report_as_at_28th_February_2025.pdf; Square Enix, abrufbar unter: https://static.square-enix-games.com/Square_Enix_DSA_Transparency_Report.pdf; Take-Two Interactive, abrufbar unter: <https://ir.take2games.com/static-files/b7784109-bccb-48df-83f6-e76bdd37b2af>; Xbox, abrufbar unter: <https://www.xbox.com/en-US/legal/xbox-transparency-report>.

²¹ InnoGames: tbd; Wooga, abrufbar unter: <https://www.wooga.com/legal/eu-digital-services-act-information-en>.

²² GamesWirtschaft, Die größten Games-Studios in Deutschland 2024, abrufbar unter: <https://www.gameswirtschaft.de/wirtschaft/groesste-games-studios-deutschland-2024-150824/>.

²³ Electronic Arts, Take-Two Interactive: Layout-Text, Wooga: Excel-Tabelle.

²⁴ Nintendo: 2 Seiten, Xbox: 38 Seiten

²⁵ EU-Kommission, Kommission harmonisiert Vorschriften für die Transparenzberichterstattung im Rahmen des Gesetzes über digitale Dienste, abrufbar unter: <https://digital-strategy.ec.europa.eu/de/news/commission-harmonisiert-transparenz-reporting-rules-inder-digital-services-act>.

²⁶ EU-Kommission, Durchführungsverordnung zur Festlegung von Mustern für die Transparenzberichtspflichten der Anbieter von Online-Plattformen, abrufbar unter: <https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-laying-down-templates-concerning-transparency-reporting-obligations>.

allem Überfluss ist der Ausfüllhinweis dafür nur auf Englisch auf der Kommissions-Webseite abrufbar. Der Prozess ist durch den neuen Meldebogen sehr unhandlich geworden. Er ist faktisch nur von spezialisierten Compliance- und Rechtsabteilungen zu bewältigen, über die viele mittelständische Spieleanbieter gar nicht verfügen. Es drängt sich die Frage auf, warum die Kommission sich für riesige und sperrige Excel-Tabellen als zwingendes Berichtsformat entschieden hat. Es wäre zielführender, wenn es für alle Anbieter ein einheitliches Online-Formular gäbe, dass je nach Anbieterart nur die relevanten Meldeinformationen abfragt.

4. Inhalt der Berichte

Auch in inhaltlicher Hinsicht ist bei den im Jahr 2024 veröffentlichten Transparenzberichten eine große Vielfalt sichtbar. Das Kernstück der Berichte sind die Angaben zu Anordnungen von Mitgliedstaaten und Meldungen von Personen und Einrichtungen gem. Art. 15 Abs. 1 lit. a und lit. b DSA. Hier müssen Anbieter die Anzahl der erhaltenen Anordnungen und Meldungen nach der Art der betroffenen mutmaßlich rechtswidrigen Inhalte aufschlüsseln. Spannend ist dabei, wie unterschiedlich die Spieleanbieter die Inhaltsarten kategorisiert haben: Bei den meisten Anbietern finden sich sinngemäß Kategorien für

- Bedrohung und Gewalt,
- Belästigung und Nachstellen,
- Betrug,
- Hassrede und
- sexuelle Inhalte.

Dagegen weisen nur vereinzelte Anbieter zB

- Cheating,
- Datenmissbrauch,
- Malware und Phishing,
- öffentliche Sicherheit und Terrorismus oder
- Spam und unerlaubte Werbung

gesondert aus. Es ist anzunehmen, dass letztere Inhaltsarten bei den Anbietern bislang gar nicht gesondert erfasst wurden oder nur als „Sonstige“ ausgewiesen wurden. Insgesamt geben die meisten Anbieter zwischen 5 und 10 Kategorien vor.

Auch hier schreitet die EU-Kommission nun mit den einheitlichen Meldebögen ein. Diese geben detailscharf die Kategorien rechtswidriger Inhalte vor. Insgesamt gibt es 15 Oberkategorien mit jeweils bis zu 7 Unterkategorien, insgesamt 99 Parameter. Diese reichen von der Oberkategorie 1 „Tierwohl“ bis zur Oberkategorie 15 „Sonstiger Verstoß gegen die Geschäftsbedingungen des Anbieters“. Zur Veranschaulichung für den Detailgrad der Unterkategorien sei hier exemplarisch die Kategorie 3 „Cybergewalt“ angeführt: Diese enthält die Unterkategorien 3a „Mobbing und Einschüchterung“, 3b „Cyberbelästigung“, 3c „Aufstachelung zu Gewalt oder Hass“, 3d „Cyberstalking“, 3e „Nicht einvernehmliche Weitergabe von intemem Material“, 3f „Nicht einvernehmliche Weitergabe von mit Deepfake-Technik bearbeitetem Material“ und 3g „Sonstiges“. Die Haupt- und Unterkategorien sind so detailscharf, dass die Transparenzberichte wie ein Erfassungsbogen einer wissenschaftlichen Langzeitstudie anmuten.

5. Kritik an Inhaltvorgaben

Diese extreme Detailschärfe stellt Spieleanbieter vor die Herausforderung, ihre bisherige interne Kategorisierung auf diesen neuen Quasi-EU-Standard umzustellen. Dies ist eine gewaltige Aufgabe, denn die meisten bestehenden Meldesysteme sind viel einfacher gestaltet. Dies kann man aus den im Jahr 2024 veröffentlichten Transparenzberichten gut ablesen, in denen die meisten Anbieter nur 5 bis 10 Oberkategorien und

keine Unterkategorien ausweisen. Tatsächlich kommen bestimmte Kategorien bei Spieleanbietern gar nicht vor: ZB sind Schneeballsysteme, Tierquälerei oder Umweltgefahren im Gaming-Kontext sehr selten, müssen in den Meldebögen aber trotzdem erfasst werden. Auch ist die Auswahl der richtigen Kategorie mitunter schwer: Etwa dann, wenn zwischen Kategorie 3 „Cybergewalt“ und Kategorie 4 „Cybergewalt gegen Frauen“ unterschieden werden muss, obwohl Spieleanbieter das Geschlecht der Spieler mangels Relevanz und wegen Datensparsamkeit regelmäßig nicht erfassen. Oder wenn zwischen den Unterkategorien 3a „Cybermobbing“, 3b „Cyberbelästigung“ und 3c „Cyberstalking“ unterschieden werden muss, obwohl die Sachverhalte oft schwammig sind und mehrere Unterkategorien betreffen.

Zudem weichen die Kategorien des Meldebogens von Kategorien in anderen Ländern ab und erzeugen damit eine Divergenzproblem. ZB sind die 99 Parameter des DSA inkongruent zu den 130 Priority Offences des UK Online Safety Act.²⁷ Zumeist sind Spieleanbieter aber in der EU und in UK gleichzeitig wirtschaftlich aktiv. Dies führt praktisch dazu, dass für EU und UK eine Parallelerfassung aller Meldungen in beiden Categoriesystemen stattfinden muss, was erheblichen Mehraufwand bedeutet. Hierbei sind andere Länder außerhalb der EU noch gar nicht bedacht, die perspektivisch eigene Gesetze betreffend Online-Gefahren erlassen wollen. Wünschenswert wäre, dass derartige Vorgaben innerhalb Europas und der OECD angeglichen werden.

Eine andere, eher juristische Herausforderung für die Spieleanbieter ist die Differenzierung nach dem Rechtsgrund aus Art. 15 Abs. 1 lit. b Alt. 3 DSA. Danach müssen Anbieter für jede infolge einer Meldung ergriffene Maßnahme differenzieren, ob diese auf Grundlage allgemeiner Gesetze oder den eigenen AGB erfolgt ist. Das ist in der Praxis oft kaum trennbar, weil die AGB zumeist den öffentlich-rechtlichen Rechtsrahmen des Sitzlandes des Anbieters spiegeln. So ist zB in Deutschland Cyberstalking inzwischen in § 283 StGB geregelt, aber auch nach den AGB der meisten Spieleanbieter verboten. Ob eine Maßnahme gegen Cyberstalking aufgrund allgemeiner Gesetze oder den eigenen AGB ergriffen wurde, lässt sich also gar nicht sagen, weil beides zutrifft.

V. Einrichtung von Melde- und Abhilfeverfahren

1. Neue Vorgaben und Stand der Umsetzung

Anbieter von Online-Spielen verfügen seit jeher über Melde- und Abhilfeverfahren für nutzergenerierte Inhalte. Neu an dem in Art. 16 DSA vorgesehenen Meldeverfahren ist, dass die Meldenden mehr eigene personenbezogene Daten mitteilen und eine Richtigkeits- und Vollständigkeitserklärung abgeben müssen. Art. 16 Abs. 2 lit. c DSA sieht die Angabe des Namens und der E-Mail-Adresse der melden Person oder Einrichtung vor. Art. 16 Abs. 2 lit. d DSA erfordert zudem eine Erklärung, dass der Meldende in gutem Glauben von der Richtigkeit und Vollständigkeit der Meldung überzeugt ist. Dies ist für die Spielbranche unüblich, denn meist nutzen Spieler statt ihrem Klarnamen ein Pseudonym. Zudem geben die Spieler bei der Registrierung für ein Online-Spiel immer seltener ihre E-Mail-Adresse gegenüber dem Spieleanbieter preis: Zunehmend erfolgt das Log-in über Plattform von Drittanbietern wie Apple (App Store), Google (Play Store), Microsoft (Xbox), Nintendo (Switch Online), Sony (Playstation), Valve (Steam), wobei die E-Mail-Adresse

²⁷ OFCOM, Overview of Illegal Harms, abrufbar unter: <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/overview-of-illegal-harms.pdf?v=390985>.

nicht an den eigentlichen Spieleanbieter weitergegeben wird. Auch ist es unüblich, bei der Meldung eine umfassende rechtliche Erklärung über Richtigkeit und Vollständigkeit abzugeben – meist genügt bisher eine formlose Meldung.

Zudem müssen gem. Art. 17 DSA Spieleanbieter ihre Abhilfeentscheidungen nun ausführlicher begründen. Verlangt wird, dass eine „klare und spezifische Begründung“ für alle Beschränkungen vorgelegt wird. Diese soll gem. Art. 17 Abs. 3 lit. a DSA die Tatsachen und Umstände, auf denen die Entscheidung beruht enthalten. Zudem soll sie gem. Art. 17 Abs. 3 lit. b DSA angeben, ob die Entscheidung auf die Meldung eines Nutzers oder freiwillige Untersuchung des Spieleanbieters auf Eigeninitiative zurückgeht und in bestimmten Fällen sogar die Identität der meldenden Person. Zwar werden Moderationsentscheidungen in Online-Spielen auch jetzt schon begründet, aber oft nur kurz und knapp. Art. 17 DSA scheint dagegen einen regelrechten „Tatbestand“ wie in Gerichtsurteilen einzufordern. Besonders kritisch ist zudem für Spieleanbieter, dass sie angeben müssen, ob die Entscheidung aus einer Nutzermeldung oder Eigenrecherche resultiert. Hier halten sich die Anbieter oft bewusst bedeckt, um ihre Erkenntnisquellen zu schützen. Das ist vor allem bei Spielbetrug (Cheating) ein Problem, dass als sonstiger Verstoß gegen die Geschäftsbedingungen des Anbieters nun dem DSA unterfällt.

2. Kritik an den Vorgaben

Die neuen Vorgaben zu Klarnamenpflicht, Adressangabe sowie Richtigkeits- und Vollständigkeitserklärung bei Inhaltsmeldungen stellen einen Bruch mit der erfolgreichen formlosen Meldekultur im Online-Spielebereich dar. Sie sind für die Spieler ein Rückschritt gegenüber dem Status quo, denn damit werden anonyme und verdachtsbasierte Meldungen erschwert bis unmöglich und die Meldenden setzen sich gegenüber den Gemeldeten einem Vergeltungsrisiko aus. Möglicherweise hat dies einen „chilling effect“ und verringert sogar die Meldezahlen. Umgekehrt führen die Vorgaben zur Begründungspflicht bei Abhilfemaßnahmen zu unnötigem Mehraufwand. Noch schlimmer ist, dass dadurch Spielbetrüger eine Ausforschungsmöglichkeit erhalten, denn sie können aus gegen sie ergangenen Abhilfeentscheidungen den Ermittlungsweg und möglicherweise sogar die Informanten ableiten. Besser wäre es, Ausnahmen von der Begründungspflicht vorzusehen, wenn dadurch die zukünftige Aufdeckung von Verstößen oder Rechtsverfolgung des Anbieters erschwert wird.

VI. Fazit

Die sich aus dem DSA ergebenden Pflichten der Spieleanbieter für die Inhaltsmoderation bedeuten einen erheblichen persönlichen, finanziellen und organisatorischen Aufwand. Ein Regelungsbedarf bestand für die Games-Branche nicht, da nahezu alle Spieleanbieter bereits seit vielen Jahren im eigenen Interesse und im Interesse der reibungslosen Nutzung der Spiele umfangreiche technische Systeme sowie Community-Management Abteilungen vorhalten, die sich darum kümmern, dass Nutzer nicht ohne Konsequenzen unerwünschte oder gefährliche Inhalte verbreiten. Aus Sicht der Spieler zu begrüßen ist der Umstand,

dass bereits in den Nutzungsbedingungen die Sanktionen für mögliche Verstöße klar festgelegt sein müssen.

Die Berichtspflichten bedeuten für die Unternehmen erhebliche Ausgaben und Personaleinsatz. Der Effekt solcher Transparenzberichte – sofern sie überhaupt gelesen werden – ist gering. Während derzeit über alle politischen Lager hinweg Bürokratieabbau gefordert wird, errichtet die EU-Regulierung beständig neue bürokratische Pflichten. Auch die zusätzlichen Anforderungen bei Melde- und Abhilfeverfahren sind kontraproduktiv. Die Meldeverfahren widersprechen dem datenschutzrechtlichen Prinzip der Datenminimierung. Zudem werden hilfreiche anonyme und verdachtsbasierte Meldungen erschwert. Bei den Abhilfemaßnahmen entsteht eine unnötig hohe Begründungslast. Dagegen ergeben sich für Spielbetrüger neue Ausforschungsmöglichkeiten.

Insgesamt ist der sich aus dem DSA ergebende Umsetzungsaufwand erheblich. Die Situation der Nutzer wird indes gegenüber dem faktischen Status quo vor Inkrafttreten des DSA kaum verbessert. Die positiven Effekte des DSA sollten nach einigen Jahren evaluiert werden, um zu entscheiden, ob man bürokratische Hürden abbaut, wenn der gewünschte Effekt der Regulierung nicht eingetreten ist.

Schnell gelesen ...

- Spieleanbieter müssen bei der Inhaltsmoderation die Transparenzpflichten aus Art. 14 bis 17 DSA erfüllen. Unter Inhaltsmoderation versteht man die Verfahren zur Überprüfung von nutzergenerierten Inhalten auf Einhaltung von AGB und öffentlichem Recht.
- Typischerweise setzen Anbieter von Spielen mit Mehrspielermodus auf ein abgestuftes Sanktionssystem: Entfernung der Inhalte, Einschränkung der Nutzungsmöglichkeit, vorübergehende Sperrung und schließlich endgültiger Ausschluss.
- Sind Personen unter 16 Jahren zugelassen, muss eine Aufbereitung der AGB in verständlicher Form erfolgen.
- Die Anforderungen an Transparenzberichte sind ein bürokratischer Albtraum.
- IRd Regelungen zu Melde- und Abhilfeverfahren stellen die neuen Vorgaben zu Klarnamenpflicht, Adressangabe und Richtigkeits- und Vollständigkeitserklärung einen Bruch mit der erfolgreichen formlosen Meldekultur im Online-Spielebereich dar.



Patrick Mitsching, LL.M. (Durham), M.A. (London), ist Leiter der Rechtsabteilung bei der InnoGames GmbH in Hamburg.



Professor Dr. Christian Rauda ist Fachanwalt für IT-Recht, Fachanwalt für Urheber- und Medienrecht, Fachanwalt für gewerblichen Rechtsschutz und Partner der Sozietät ARTANA in Hamburg sowie Professor für Computerspielrecht und Entrepreneurship in der Games-Branche an der HTW Berlin.

Neue Compliance-Anforderungen für ein sicheres digitales Ökosystem

Empfehlungen für Spieleentwickler und Plattformbetreiber

Compliance-Management-System

Der Digital Services Act (DSA) markiert einen grundlegenden Wandel in der Regulierung digitaler Dienste und stellt insbesondere die Gaming-Branche vor neue Anforderungen an ihr Compliance-Management. Mit seinem differenzierten Regulierungsansatz – von reinen Durchleitungsdiensten über Online-Plattformen bis hin zu Suchmaschinen – verfolgt der DSA das Ziel, ein sicheres digitales Ökosystem zu schaffen und illegale Inhalte wirksam einzudämmen. In der Praxis zeigt sich er-

freulicherweise, dass zentrale Elemente der DSA-Vorgaben bereits weitgehend von führenden Plattformanbietern und Betreibern von Online-Spielen antizipiert und implementiert wurden. Dazu zählen u.a. interne Prozesse und Richtlinien, Melde- und Beschwerdemechanismen, umfangreiche Transparenzpflichten sowie spezifische Verpflichtungen für sehr große Online-Plattformen.

Lesedauer: ●● Minuten

I. Einleitung

Der Digital Services Act (DSA) verfolgt einen abgestuften Regulierungsansatz je nach Funktion und Größe des Diensteanbieters. Erfasst werden nach Art. 3 DSA reine Durchleitungsdienste, Caching-Dienste, Hosting-Dienste, Online-Plattformen und Online-Suchmaschinen. Im Bereich Games sind dies Plattformen wie Steam, Origin, Playstation Network, Xbox Gaming, Nintendo eShop, Epic Store, aber auch Kommunikationsplattformen wie Discord und TeamSpeak.

Der europäische Gesetzgeber hat die Relevanz des DSA für Computer- und Videospiele ausdrücklich anerkannt und in seiner Entschließung zum Binnenmarktkonzept für den Verbraucherschutz bei Online-Videospielen v. 18.1.2023 die Schaffung eines sicheren digitalen Umfelds sowie die zügige Anwendung des DSA im Hinblick auf die Verbreitung illegaler Inhalte über spielinterne Kommunikationsfunktionen gefordert¹.

Eine der wichtigsten Anforderungen des DSA ist die Unterhaltung eines Compliance-Management-Systems (CMS). In der eher mittelständisch geprägten Games-Branche ist das Thema Compliance, wie generell im Mittelstand, eher unterentwickelt. Vor diesem Hintergrund lohnt sich ein Blick auf die wichtigsten Aspekte des DSA in Bezug auf Compliance.

II. Grundsätze des DSA-Compliance-Managements

Zunächst lohnt sich ein Blick auf die generelle Struktur von Compliance-Management-Systemen (CMS)². Dazu gehören die Festlegung von Regeln und Prozessen, die Einführung einer Organisationsstruktur, die Schulung und Sensibilisierung der Mitarbeiter und schließlich die Überwachung und kontinuierliche Verbesserung des CMS.

1. Implementierung interner Prozesse und Richtlinien

Zur Umsetzung der Vorgaben des DSA sollten Anbieter digitaler Dienste zunächst interne Prozesse und Richtlinien implementieren. Diese dienen der effektiven Moderation von Inhalten, der Transparenz sowie der rechtssicheren Kommunikation mit Nutzern und Behörden³.

Eine weitere wichtige Anforderung an die erfassten Diensteanbieter ist die Einrichtung eines Melde- und Abhilfeverfahrens zur Entfernung rechtswidriger Inhalte gem. Art. 16 DSA. Dazu gehört die Erstellung transparenter und leicht verständlicher Richt-

linien, die festlegen, welche Inhalte als rechtswidrig gelten und unter welchen Bedingungen sie entfernt oder gesperrt werden. Die Moderation soll sich an geltendem EU-Recht und nationalen Vorschriften orientieren, insbesondere in Bereichen wie Hassrede, Terrorismuspropaganda und Urheberrechtsverletzungen. Um eine effiziente Umsetzung sicherzustellen, müssen standardisierte Prüfverfahren eingeführt werden, mit denen illegale Inhalte identifiziert, bewertet und entfernt werden können. Dabei ist sowohl die Schulung von Moderationsteams als auch der Einsatz automatisierter Systeme erforderlich, um eine schnelle und präzise Bearbeitung zu gewährleisten⁴.

Games-Anbieter sollte dies vor keine größeren Herausforderungen stellen. Community-Guidelines und Spielregeln einschließlich Anti-Cheat-Richtlinien sind gängige Standards, insbesondere bei Online-Multiplayer-Games.

Ein weiterer zentraler Punkt ist die Einrichtung eines Beschwerdemechanismus für Nutzer gem. Art. 20 DSA. Plattformen müssen ein benutzerfreundliches Meldeverfahren bereitstellen, über das Nutzer illegale Inhalte melden können. Eine schnelle und nachvollziehbare Bearbeitung dieser Meldungen durch ein geschultes Moderationsteam ist essenziell⁵. Darüber hinaus muss ein Beschwerdemechanismus eingerichtet werden, über den betroffene Nutzer Einspruch gegen Entscheidungen zur Entfernung oder Einschränkung ihrer Inhalte einlegen können. Transparenz spielt dabei eine wichtige Rolle: Nutzer müssen über getroffene Entscheidungen, deren Begründung und mögliche Einspruchsmöglichkeiten informiert werden. In bestimmten Fällen kann ein externes Streitbelegungsverfahren angeboten werden, um eine unabhängige Überprüfung von Moderationsentscheidungen zu ermöglichen⁶.

Auch hier sollten zumindest die technischen Voraussetzungen für Games-Anbieter keine größeren Hürden darstellen. Die Games-Branche ist ein Pionier bei der Zielgruppenkommunikation über das Internet. Spätestens mit dem Siegeszug der Online-Spiele Mitte der 2000er-Jahre und der Online-Fähigkeit der wichtigsten Gaming-Plattformen stehen Anbieter und Spieler

¹ Entschließung des Europäischen Parlaments zum Binnenmarktkonzept für den Verbraucherschutz in Online-Videospielen (2022/2014 (INI)), dort Ziff. 46.

² Zu Compliance Strukturen detailliert: Goette/Barring DStR 2021, 1238 ff.

³ S. Erwägungsgrund 5 DSA.

⁴ Ausf. Mitsching/Rauda MMR 2025, ●●● – in diesem Heft.

⁵ Vgl. Erwägungsgrund 58 DSA.

⁶ Erwägungsgrund 149 DSA nennt explizit Verbandsklagen und Verbraucherschutzverbände.

über Nutzerkonten in direktem Kontakt, um auch Beschwerden und Supportanfragen direkt zu bearbeiten.

Zur Sicherstellung der Nachvollziehbarkeit und Einhaltung der DSA-Vorgaben treffen Diensteanbieter konkrete Transparenzberichtspflichten und damit verbundene Verfahren zur Dokumentation und Berichterstattung nach Art. 15 und 42 DSA. Hierzu gehört die Einführung eines standardisierten Dokumentationsprozesses zur Erfassung aller Moderationsentscheidungen. Erfasst werden u.a. die Anzahl und Art der gemeldeten Inhalte, die Entscheidungen zur Entfernung oder Beibehaltung von Inhalten, die Ergebnisse von Beschwerden sowie der Einsatz automatisierter Systeme zur Inhaltsmoderation. Die Unternehmen sind verpflichtet, regelmäßige Transparenzberichte zu erstellen, die öffentlich zugänglich gemacht werden und die Einhaltung der DSA-Vorgaben belegen. Zudem erfolgt eine enge Zusammenarbeit mit Aufsichtsbehörden und digitalen Dienste-Koordinatoren (Digital Service Coordinator – DSC), um eine rechtskonforme Berichterstattung sicherzustellen.

Ausgenommen von der Verpflichtung werden nach Art. 19 DSA Klein- oder Kleinstunternehmen. Nach der Empfehlung der EU-Kommission (2003/361/EG) zur Definition von Kleinstunternehmen, kleinen und mittleren Unternehmen (EU-KMU-Definition) ist ein Unternehmen ein KMU, wenn es weniger als 250 Personen beschäftigt und entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielt oder eine Jahresbilanzsumme von max. 43 Mio. EUR aufweist. Hierunter dürften ca. 99% der auf dem deutschen Markt tätigen Unternehmen zählen.

Dennoch sollten auch diese Unternehmen vor dem Hintergrund des Hinweisgeberschutzgesetz (HinSchG) ein Beschwerdemanagement unterhalten, da das HinSchG bereits ab einer Mitarbeiterzahl von 50 ein Hinweisgebersystem erforderlich macht.

2. Compliance-Organisation

Jedes funktionierende CMS sieht auch die sinnvolle Ausgestaltung einer Compliance-Organisation vor. Dabei gibt es keine gesetzlich vorgesehene oder übliche Struktur, die umgesetzt werden müsste. Da Compliance durch zahlreiche Faktoren beeinflusst wird, sollten Organisation, Maßnahmen und Kontrollsysteme an das Unternehmen angepasst sein und dessen konkreten Bedürfnissen Rechnung tragen⁷.

In der Praxis werden die Aufgaben entweder durch eine neu geschaffene Compliance-Funktion oder einen dezidiert benannten Beauftragten innerhalb bestehender Strukturen übernommen werden⁸. Die Compliance-Funktion sollte direkt an die Unternehmensleitung berichten und ist für die Einhaltung und Überwachung der DSA-Konformität verantwortlich. Sie wird darüber hinaus eine effektive Zusammenarbeit zwischen verschiedenen Abteilungen sicherstellen, zB der Rechtsabteilung, die die Umsetzung der rechtlichen Verpflichtungen aus dem DSA, insbesondere Melde- und Sorgfaltspflichten auf der Governance-Ebene übernimmt, der IT-Abteilung, die die Implementierung von Mechanismen zur Transparenz von Algorithmen und Risikobewertungen übernehmen wird, die Funktion Content-Moderation soll die Sicherstellung fairer und objektiver Moderationsentscheidungen gemäß den Vorgaben der Art. 16 bis 20 DSA übernehmen und schließlich wird der Datenschutzbeauftragte einzubeziehen sein, der die Abstimmung mit Da-

tenschutzvorgaben im Zusammenhang mit der DS-GVO übernehmen sollte.

Die Unternehmen der Games-Branche sind regulierungserfahren. Neben Jugendschutzaufgaben gibt es auch zahlreiche verbraucherschutzrechtliche Implikationen bei Games, sodass es sinnvoll erscheint, die Compliance-Funktion an bestehende Strukturen anzubinden.

Besondere Anforderungen an die Compliance-Organisation sieht Art. 41 DSA allerdings bei sehr großen Online-Plattformen (Very Large Online Platforms – VLOPs) und sehr großen Online-Suchmaschinen (Very Large Online Search Engines – VLOSEs). Diese Unternehmen müssen eine explizit unabhängige Compliance-Funktion einrichten, um die Einhaltung der gesetzlichen Vorgaben sicherzustellen. Plattformen mit mehr als 45 Mio. monatlich aktiven Nutzern in der EU gelten als VLOPs. Bisher hat die EU noch keine Spieleplattform als VLOP eingestuft. Vor diesem Hintergrund dürfte die Unabhängigkeit der Compliance-Funktion eine Struktur außerhalb der normalen Berichtslinie erfordern.

Allerdings dürften in der Spieleindustrie nur sehr wenige Unternehmen als VLOPs einzustufen sein. Das PlayStation Network (PSN) wird Ende 2024 weltweit insgesamt 129 Mio. monatlich aktive Nutzer haben. Je nach Anteil der EU am Gesamtmarkt dürfte die Marke von 45 Mio. Nutzern bald erreicht werden. Für Xbox Gaming von Microsoft werden ähnlich hohe Nutzerzahlen erwartet.

3. Schulungen und Sensibilisierung

Neben einer adäquaten Compliance-Organisation ist ein weiterer wichtiger Bestandteil eines jeden CMS ist ein Schulungs- und Trainingsprogramm.⁹ Der DSA trägt diesem Umstand Rechnung und sieht die stetige Schulung von Mitarbeitern vor, um diese für die regulatorischen Anforderungen zu sensibilisieren¹⁰. Art. 15 und 42 DSA fordern sogar, die Schulungsmaßnahmen der Mitarbeiter in den Transparenzbericht aufzunehmen.

Besonders im Bereich der Content-Moderation und der technischen Umsetzung des DSA sind fundierte Kenntnisse über rechtliche Vorgaben und die jeweiligen eigenen Plattformrichtlinien unerlässlich. Daher sollten Unternehmen kontinuierliche Schulungsprogramme etablieren, um sicherzustellen, dass ihre Teams die notwendigen Kompetenzen zur korrekten Anwendung der Moderationsrichtlinien und zur Umsetzung rechtlicher Verpflichtungen besitzen. Diese Schulungen sollten praxisnah gestaltet sein und sowohl die Identifikation und Entfernung illegaler Inhalte als auch das Beschwerdeverfahren selbst gemäß den Vorgaben des DSA umfassen. Dies dürfte zu den inhaltlichen Fragen hinzukommen.

Im Bereich Games dürften die Übergänge zwischen Support und Content-Moderation fließend sein. Insbesondere bei Games mit integrierten Chatfunktionen, wie sie zB die meisten Ego-Shooter aufweisen, sind Beschwerdemöglichkeiten häufig bereits implementiert, um Flaming, Cheating oder auch die Verwendung von rechtswidrigen Symbolen zu unterdrücken. Darüber hinaus werden bei Online-Spielen bereits technische Systeme verwendet, um rechtswidrige nutzergenerierte Inhalte sowie Betrugssoftware zu erkennen und zu blockieren.

Neben technischen und rechtlichen Aspekten sollte die Schulung auch ethische Fragestellungen einbeziehen, insbesondere im Hinblick auf den Schutz der Meinungsfreiheit und den verantwortungsvollen Umgang mit automatisierten Entscheidungsprozessen. Ein weiterer Schwerpunkt liegt auf der Sensibilisierung für Algorithmentransparenz und den verantwortungsvollen Einsatz von KI-gestützter Moderation, wie in Art. 27 DSA gefordert¹¹.

⁷ Kramer, IT-ArbR/Schulze/Zumkley, 3. Aufl. 2023, § 2 Rn. 996.

⁸ Ausf. zur Ausgestaltung der Compliance-Organisation Hoffmann/Schieffer NZG 2017, 404.

⁹ S. zu Compliance-Schulungen Kramer, IT-ArbR/Schulze/Zumkley, 3. Aufl. 2023, § 2 Rn. 1066.

¹⁰ Vgl. hierzu Erwägungsgrund 87 DSA.

¹¹ Ausf. in Erwägungsgrund 70 DSA.

Die Mitarbeiter sollen verstehen, wie algorithmische Systeme zur Erkennung, Filterung und Moderation von Inhalten eingesetzt werden und welche potenziellen Risiken damit verbunden sind, insbesondere in Bezug auf Diskriminierung, Fehleinschätzungen oder Intransparenz. Zudem sollten sie darin geschult werden, wie algorithmische Entscheidungen überprüft und ggf. korrigiert werden können, um eine faire und rechtskonforme Inhaltsmoderation sicherzustellen.

4. Kontinuierliche Überwachung und Verbesserung

Schließlich erfordert ein wirksames Compliance-Management eine kontinuierliche Überwachung und Verbesserung der bestehenden Strukturen und Prozesse, um etwaige Schwachstellen zu erkennen und zu schließen¹². Ein zentraler Bestandteil dieses Prozesses ist deshalb die Implementierung eines Kontrollsystems, das eine systematische Überwachung und Überprüfung der eingeführten Compliance-Maßnahmen ermöglicht. Die Richtlinien und Verfahren zur Inhaltsmoderation, Transparenz und Nutzerschutz sollten sowohl automatisiert als auch manuelle überprüft werden. Werden Defizite oder Qualitätsmängel festgestellt, sind diese umgehend abzustellen und zu optimieren.

III. DSA-Compliance-Pflichten nach Plattformtyp in der Games-Industrie

Die weiteren spezifischen Compliance-Anforderungen des DSA sind ferner gestaffelt und richten sich nach der Art und Größe der digitalen Dienste¹³.

1. Allgemeine Verpflichtungen für alle digitalen Dienste

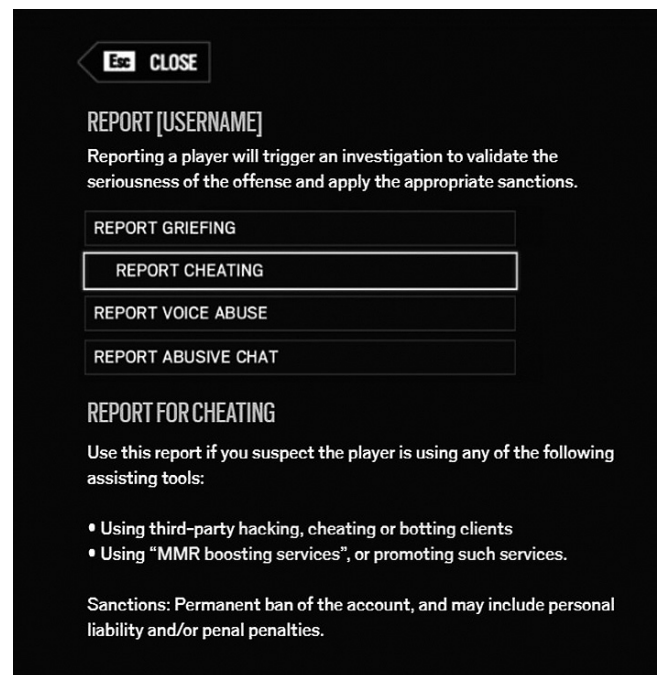
Für alle digitalen Dienste gelten zunächst Verpflichtungen, die insbesondere der Transparenz- und Meldepflichten umfassen. So müssen alle Anbieter gem. Art. 11 und 12 DSA eine leicht zugängliche Kontaktstelle für Behörden und Nutzer einrichten, über die rechtliche Anfragen und Beschwerden eingereicht werden können.

Anbieter, die in der Union keine Niederlassung haben, sind nach Art. 13 DSA verpflichtet, einen gesetzlichen Vertreter zu benennen. Dies soll die Kommunikation erleichtern und hat vor allem für Nicht-EU-Anbieter große praktische Relevanz im Hinblick auf Zustellungs- und Vollzugsfragen bei behördenkontakt. Die Kontaktstelle soll eine beidseitige Kommunikation ermöglichen, muss also mehr sein als eine einfaches Kontaktformular¹⁴. Ein Beispiel hierfür wäre ein Spieleentwickler, der ein Multiplayer-Game betreibt und eine Support-Hotline oder ein Online-Funktion bereitstellt, über das Nutzer Verstöße oder Sicherheitsprobleme melden können. Dies ist bereits gängige Praxis und damit keine größere Herausforderung für die Anbieter.

Der französische Anbieter Ubisoft unterhält zB Kommunikations- und Beschwerdemechanismen sowohl auf ihrer Internetwebseite¹⁵ als auch direkt implementiert in vielen Online-Spielen¹⁶. In den Spielen selbst gibt es die Möglichkeit, die „Mitspieler“ live online zu melden, zB durch die Auswahl der Funktion „Spieler anzeigen“ und nach dem Auswählen sodann die Voreinstellung „Spieler melden“.

In Ubisofts Ego-Shooter Rainbow Six Siege sieht das Meldesystem im Spiel zB so aus, wie in der Abbildung dargestellt.

Das Verfahren sowie die Konsequenzen der Meldungen werden beschrieben und außerdem bietet das Meldesystem eine Auswahl potenzieller Verstöße wie Cheating oder rechtswidrige Chats. Hierdurch werden Meldungen erleichtert und Nutzer motiviert, die Einhaltung der Community-Regeln zu selbst zu



Quelle: Ubisoft

kontrollieren. Gleichzeitig dürften die Vorgaben auch den beschriebenen gesetzlichen Anforderungen genügen.

Zudem sind Unternehmen verpflichtet, gem. Art. 15 DSA jährlich einen Transparenzbericht zu veröffentlichen, der u.a. darlegt, welche Moderationsmaßnahmen gegen rechtswidrige oder unangemessene Inhalte ergriffen wurden. In der Gaming-Branche könnte dies die Veröffentlichung von Statistiken über gesperrte Nutzerkonten aufgrund von Hatespeech, Betrugsversuchen oder anderen Verstößen innerhalb einer Online-Community umfassen.

Auch hier sind insbesondere die größeren Unternehmen bereits aktiv. Microsoft veröffentlicht bereits seit 2022 einen Xbox Transparenzbericht¹⁷. In diesem Bericht gibt Microsoft umfassend Auskunft über alle Aktivitäten im Zusammenhang mit der Xbox Gaming Plattform und den Spielen der Xbox Game Studios wie Age of Empires und Minecraft und Halo. Dabei werden sowohl Definitionen, Richtlinien und Guidelines verknüpft¹⁸. Interessant sind die geteilten Statistiken, die einen Einblick in die Datenflut geben, die es zu moderieren gilt. Laut Transparenzbericht 2024 hat Microsoft von Februar bis Dezember 2024 insg. 17,2 Mrd. Inhalte moderiert¹⁹. Zu den Inhalten zählt Microsoft Texte, Usernamen, Bilder und sonstige nutzergenerierte Inhalte auf den Plattformen, laut Bericht wurden insgesamt 409 Mio. Inhalte (2,4%) als unzulässig qualifiziert. Davon wurden 209 Mio. als Missbrauch der Plattformen klassifiziert, 54 Mio. Inhalte wurden als Obszönität und Vulgarität eingeordnet und 46 Mio. als Pornografie, 32 Mio. Inhalte als Mobbing und Belästigung sowie 27 Mio. als „Hatespeech“. Der Inhalt wird automatisiert überwacht und erfasst. Allerdings wurden auch Missstände berichtet. Microsoft erhielt im Berichtszeitraum 53,2 Mio. Meldun-

¹² Goette/Barrington sprechen zutreffend von einer „Pflicht zur nachfolgenden Reflexion des Compliance-Management-Systems“, DStR 2021, 1240.

¹³ Ausf. Kraul/Schmidt CCZ 2023, 177.

¹⁴ Erwägungsgrund 42 DSA.

¹⁵ Abrufbar unter: <https://www.ubisoft.com/de-de/help/contact>.

¹⁶ Exemplarisch abrufbar unter: <https://www.ubisoft.com/de-de/help/the-division-2/gameplay/article/blocking-players-in-the-division-2/000064952>.

¹⁷ Transparency Report 2024, abrufbar unter: <https://www.xbox.com/de-DE/legal/xbox-transparency-report>.

¹⁸ Abrufbar unter: <https://www.microsoft.com/en-ca/DigitalSafety/policies>.

¹⁹ S. dazu S. 20 des Transparency Reports 2024.

gen, die in 9,2% der Fälle (5 Mio.) zu Maßnahmen führten²⁰. Auch in Bezug auf die erhaltenen Meldungen setzt Microsoft auf Technologie und macht dies im Bericht transparent: „Wir bei Xbox sind davon überzeugt, dass Automatisierungen und der Einsatz von KI-gestützten Lösungen wie „Community Sift“ in Kombination mit menschlichem Fachwissen eine entscheidende und sich ergänzende Rolle bei der effektiven Identifizierung, Meldung und Verhinderung von Schäden in großem Umfang spielen, insbesondere da diese Online-Schäden technologisch immer ausgefeilter werden. Sie verhindern nicht nur, dass unerwünschte Inhalte Spieler erreichen, sondern reduzieren auch die Konfrontation von Menschen mit sensiblen Inhalten und helfen dabei, die Moderation durch Menschen auf differenziertere und komplexere Probleme zu konzentrieren.“

Die Statistiken sind beeindruckend: Im Berichtszeitraum wurden 1 Mio. Meldungen händisch geprüft, 4 Mio. automatisch verarbeitet. Weitere 12 Mio. Inhalte durchliefen zunächst einen automatisierten Scan und wurden anschließend manuell kontrolliert. Insgesamt erfasste und analysierte das System 400 Mio. Beiträge vollständig automatisiert.“

2. Zusätzliche Anforderungen für Hosting-Dienste und Online-Plattformen

Hosting-Dienste und Online-Plattformen unterliegen zusätzlichen Anforderungen, insbesondere hinsichtlich Inhaltsmoderation und Beschwerdebearbeitung.

Nach Art. 16 DSA müssen Anbieter ein nutzerfreundliches Meldesystem implementieren, mit dem rechtswidrige Inhalte wie Hassrede oder Urheberrechtsverstöße melden können. Damit existieren jetzt europaweit einheitliche Vorgaben für ein Notice-and-Takedown-Verfahren, um die elektronische Meldung von Inhalten als illegal zu ermöglichen. Bedauerlich ist das Fehlen einer Binnenkollisionsnorm, die Klarheit in Bezug auf das jeweils anwendbare Recht gibt. In Art. 3 lit. h DSA sind Inhalte als rechtswidrig definiert, wenn sie „nicht im Einklang mit dem Unionsrecht oder dem Recht eines Mitgliedstaats stehen“.

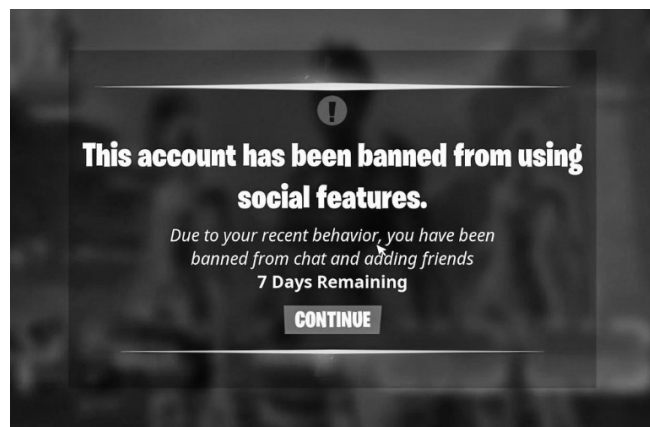
Für die Games-Industrie ändert sich der Status quo, zB in Bezug auf verfassungsfeindliche Symbole oder den Jugendschutz, nicht. Aufgrund der fragmentierten europäischen Regulierung, zB im Jugendschutz, hat die Branche bereits eigenständig europäische einheitliche Standards etabliert²¹ und dürfte deshalb einheitliche europäische Regelungen begrüßen.

Zudem verlangt Art. 20 DSA einen internen Beschwerdemechanismus, der es betroffenen Nutzern ermöglicht, Moderationsentscheidungen anzufechten. Dies könnte bedeuten, dass ein Spieler, dessen Konto wegen angeblicher Verstöße gesperrt wurde, die Möglichkeit erhält, Einspruch einzulegen und eine erneute Überprüfung durch einen Moderator zu beantragen. Auch insoweit verfügen die Anbieter von Online-Spielen bereits über etablierte Mechanismen, die idR über die obligatorischen Nutzeraccounts geführt werden und entweder in den Spielen selbst angesteuert werden können oder über das Anbieterportal. Die Sanktionen können zeitlich befristet oder dauerhaft ausgestaltet sein.

Maßnahmen gegen Missbrauch spielen ebenfalls eine wichtige Rolle. Plattformen müssen gem. Art. 23 DSA Nutzer identifizieren und ggf. sperren, wenn diese wiederholt gegen Plattformrichtlinien oder gesetzliche Vorgaben verstoßen. In der Games-Industrie ist dies insbesondere für Online-Spiele mit hohen Mo-

²⁰ S. 22 des Transparency Reports 2024.

²¹ S. für den Jugendschutz zB PEGI, das Pan European Game Information System, das länderübergreifend einen Jugendschutzstandard definiert hat.



Quelle: Epic Games

derationsanforderungen relevant, zB in Titeln wie „League of Legends“ oder „Call of Duty“, wo Entwickler Maßnahmen gegen Cheating und toxisches Verhalten etabliert haben und in der Praxis umsetzen.

Zudem verpflichtet Art. 30 DSA Plattformbetreiber, eine risikobasierte Prüfung von Anbietern auf Online-Marktplätzen durchzuführen. Dies betrifft zB Plattformen wie den Steam-Marktplatz oder den Epic Games Store, wo Drittanbieter digitale Inhalte verkaufen. Hier müssten die Anbieter sicherstellen, dass Verkäufer keine gefälschten oder illegale Inhalte vertreiben. Da die meisten Anbieter hier schon unter qualitativen Gesichtspunkten weitreichende Approval-Prozesse implementiert haben, werden sollte es auch diesbezüglich keine neuen oder gesteigerten Anforderungen aus dem DSA erwachsen.

3. Strenge Anforderungen für sehr große Online-Plattformen

Für VLOPs gelten besonders strenge Anforderungen, da sie durch ihre Reichweite potenziell größere gesellschaftliche Risiken bergen. So müssen Plattformen gem. Art. 34 DSA eine jährliche Risikobewertung durchführen, um systemische Risiken wie die Verbreitung von Desinformation oder algorithmische Verzerrungen zu identifizieren. Ein Beispiel in der Games-Branche wäre eine große Plattform wie Twitch, die überprüfen muss, ob ihre Empfehlungssysteme Hassrede oder extremistische Inhalte begünstigen. Zur Risikominderung fordert Art. 35 DSA, dass Anbieter gezielte Gegenmaßnahmen entwickeln, etwa durch verstärkte Moderation oder Anpassung der Algorithmen.

Ein weiterer wichtiger Aspekt ist die Transparenz von Empfehlungssystemen. Plattformen müssen gem. Art. 27 DSA die Funktionsweise ihrer Empfehlungsalgorithmen offenlegen. Dies betrifft zB Gaming-Plattformen, die algorithmisch generierte Spielempfehlungen basierend auf Nutzerverhalten ausspielen. Zudem müssen gem. Art. 38 DSA alternative Sortierungsoptionen bereitgestellt werden, damit Nutzer etwa zwischen einer algorithmisch sortierten und einer chronologischen Anzeige wählen können. Ein Beispiel wäre die Implementierung eines Filters in digitalen Spiele-Shops, der es Nutzern ermöglicht, Spiele unabhängig von KI-basierten Empfehlungen nach Veröffentlichungsdatum oder Beliebtheit zu sortieren.

Schließlich unterliegen VLOPs einer verstärkten externen Kontrolle. Sie sind gem. Art. 37 DSA verpflichtet, unabhängige jährliche Audits durchzuführen, um die Einhaltung der DSA-Vorgaben sicherzustellen. In der Games-Industrie könnten große Plattformen wie Xbox Live oder Discord auch unabhängige Prüfungen ihrer Moderationspraktiken durchführen lassen. Darüber hinaus müssen Plattformbetreiber nach Art. 40 DSA zugelassenen Forschern Daten zur Untersuchung von Online-Risiken

bereitstellen. Dies könnte zB die Analyse toxischer Spielerverhalten oder algorithmisch geförderter Desinformation in Multiplayer-Spielen umfassen.

Die gestaffelten Compliance-Anforderungen des DSA haben somit direkte Auswirkungen auf die Games-Industrie. Während kleinere Entwickler grundlegende Transparenzpflichten erfüllen müssen, sind große Gaming-Plattformen erheblich stärker reguliert, insbesondere hinsichtlich Inhaltsmoderation, Algorithmustransparenz und Missbrauchsverhinderung. Eine konsequente Umsetzung dieser Vorgaben kann dazu beitragen, digitale Spielplattformen sicherer, transparenter und fairer für alle Nutzer zu gestalten.

IV. Praktische Umsetzung eines DSA-Compliance-Management-Systems

Die praktische Umsetzung eines effektiven DSA-CMS erfordert eine strukturierte Herangehensweise, die sowohl technische als auch organisatorische Maßnahmen umfasst. Ein gut implementiertes CMS stellt sicher, dass alle Vorgaben des DSA in Bezug auf Transparenz, Inhaltsmoderation und Risikomanagement eingehalten werden und sollte die bestehenden Strukturen und Prozesse ergänzen. Gerade für KMUs sollte mit Augenmaß agiert werden und kein überbordender Aufwand betrieben werden.

Die Compliance-Struktur und -Governance kann hierbei an die bestehenden Strukturen angeknüpft werden. Rechtsabteilung, Personalabteilung und Customer Support sind hierbei wohl die beste Wahl. Kleinere Unternehmen, die diese Funktionen auch auslagern, zB an eine Kanzlei oder steuerlichen Berater. Vorbild kann hier Lösung der Anforderungen aus der DS-GVO, die häufig auch ausgelagert wurden.

Die Benennung eines Compliance-Beauftragten erscheint vor diesem Hintergrund sinnvoll. Dieser sollte sich regelmäßig mit den relevanten internen Abteilungen, wie der Rechtsabteilung, der Product-Abteilung und der Content-Moderation, sowie externen Beratern abzustimmen, um sicherzustellen, dass sowohl gesetzliche Anforderungen als auch Best Practices beachtet werden.

Technische und organisatorische Maßnahmen können ebenfalls an bestehende und etablierte Strukturen angeknüpft werden. Die Implementierung automatisierter Filter- und Moderationstools ist als „Profanity filter“ technisch schon lange Standard bei Online-Spielen²². Diese Tools sind heute mit KI und maschinellem Lernen ausgestattet, um automatisch problematische Inhalte zu identifizieren und umgehend zu blockieren. Die Games-Industrie hat als Pionier-Industrie deshalb bereits lange Erfahrung damit, toxisches Verhalten in Chats oder Foren zu erkennen und sofortige Maßnahmen wie temporäre Sperrungen von Nutzern zu ergreifen.

Die lückenlose Dokumentation und Berichterstattung von Beschwerdeverfahren und Abhilfemaßnahmen iSd DSA dürfte im Gegensatz zu den vorstehenden Aspekten eine neue Aufgabenstellung darstellen. Zwar veröffentlichen einige Unternehmen wie Microsoft²³ bereits seit einigen Jahren Transparenzberichte zu ihren Aktivitäten, jedoch kann dies noch nicht als Standard angenommen werden.

Nach Art. 42 DSA müssen alle Moderationsentscheidungen nachvollziehbar dokumentiert werden, sodass sie bei Bedarf überprüft werden können. Dies betrifft insbesondere die Gründe für die Entfernung von Inhalten, die Sperrung von Nutzerkonten und die Nutzung automatisierter Moderationstools. In der Games-Industrie bedeutet dies, dass jede Entscheidung über die Sperrung eines Accounts aufgrund von Cheating oder toxi-

chem Verhalten detailliert in einem System erfasst wird, das sowohl interne Teams als auch externe Prüfer auf Anfrage einsehen können. Einige Anbieter haben hier bereits technische Lösungen implementiert, die den Anforderungen des DSA entsprechen. Dabei wird sehr häufig die Information und Dokumentation über den Nutzer-Account abgebildet. Auch insoweit hat die Games-Industrie aufgrund ihrer kundenzentrierten Geschäftsmodells im Onlinebereich bereits eine gute Grundlage zur Erfüllung der Vorgaben des DSA.

V. Sanktionen

Das DSA sieht nicht nur neue Regelungen, sondern auch Sanktionen vor. Zuständig für die Verhängung sind die nationalen Koordinierungsstellen oder die EU-Kommission²⁴.

Art. 52 DSA überträgt den Mitgliedstaaten und damit den nationalen Koordinierungsstellen die Zuständigkeit für Sanktionen bei Verstößen gegen den DSA, basierend auf den Befugnissen nach Art. 51 DSA. Die Mitgliedstaaten sollen hierfür eigene Vorschriften erlassen, wobei die Sanktionen wirksam, verhältnismäßig und abschreckend sein sollen und sich nach Art, Schwere und Dauer des Verstoßes sowie der wirtschaftlichen Leistungsfähigkeit des Anbieters richten. Das deutsche Digitale-Dienste-Gesetzes (DDG) fasst in § 33 DDG insgesamt 54 Bußgeldtatbestände zusammen²⁵. Die meisten dieser Ordnungswidrigkeiten können bereits bei fahrlässigem Verhalten geahndet werden – lediglich Verstöße nach § 33 Abs. 4 DDG setzen Vorsatz voraus (§ 10 OWiG). Die Höhe der Bußgelder variiert je nach Schwere des Verstoßes, von 300.000 EUR bis hin zu 6% des weltweiten Jahresumsatzes im letzten Geschäftsjahr, insbesondere bei DSA-Verstößen durch juristische Personen mit einem Umsatz von mind. 5 Mio. oder 10 Mio. EUR.

Neben den nationalen Behörden ist auch die EU-Kommission befugt, Geldbußen und Zwangsgelder gegen VLOPs und VLSOs zu verhängen (Art. 74, 76 DSA). Bei schwerwiegenden Verstößen werden Geldbußen von bis zu 6% des weltweiten Jahresumsatzes verhängt, während bei weniger schwerwiegenden Verstößen Geldbußen von bis zu 1% des weltweiten Jahresumsatzes verhängt werden können. Sanktioniert werden vorsätzliche oder fahrlässige Verstöße gegen den DSA, gegen einstweilige Maßnahmen oder bindende Verpflichtungszusagen. Gem. Art. 74 Abs. 3 DSA ist vor der Sanktionierung eine vorläufige Beurteilung durch die Kommission erforderlich. Bei der Bemessung der Maßnahme werden insbesondere Art, Schwere, Dauer und Wiederholung der Verstöße berücksichtigt. Die Verhältnismäßigkeit der Maßnahme ist zu wahren, ebenso das Verbot der Doppelbestrafung. Gem. Art. 77 DSA können Zwangsgelder bis zu 5% des durchschnittlichen weltweiten Tagesumsatzes betragen und dienen der Durchsetzung bestimmter Maßnahmen gem. Art. 74 Abs. 1 DSA. Geldbußen und Zwangsgelder unterliegen einer fünfjährigen Verjährungsfrist gem. Art. 77 Abs. 1, 78 Abs. 1 DSA.

VI. Zusammenfassung und Ausblick

Die Digitalisierung von Öffentlichkeit und Kommunikation schreitet unaufhaltsam voran – insbesondere in der Games-Industrie, in der digitale Plattformen nicht nur Spielräume, sondern auch soziale Interaktionsräume schaffen. Mit dem Inkrafttreten des DSA im Jahr 2024 reagiert der europäische Gesetzgeber auf diesen Strukturwandel und etabliert ein einheitliches Re-

²² ZB beim Ego-Shooter Battlefield 5, abrufbar unter: <https://www.ign.com/article/s/2018/09/07/battlefield-5s-profanity-filter-is-a-work-in-progress-ea-says>.

²³ S. Transparency Report 2024.

²⁴ Ausf. Taeger/Pohle, Computerrechts-HdB/Paschke/Wernicke, 39. EL April 2024, Teil 12, 120.4 Rn. 88.

²⁵ S. Kraul GRUR-Prax 2024, 529.

gelwerk für Plattformverantwortung, Nutzerrechte und digitale Sicherheit. Die Anforderungen betreffen nicht nur klassische soziale Netzwerke, sondern zunehmend auch Gaming-Plattformen und Entwicklerstudios, die Hosting- oder Vermittlungsdienste bereitstellen.

Besonders Plattformen mit hohen Nutzerzahlen – etwa Multiplayer-Hubs, Spiele mit umfangreichen Community-Funktionen oder Livestreaming-Dienste – müssen sich auf komplexe Prüfpflichten und mögliche Kontrollen durch nationale Aufsichtsbehörden oder sogar die EU-Kommission einstellen.

Unternehmen der Games-Branche, die noch keine Compliance-Mechanismen implementiert haben, sollten jetzt handeln und ein robustes, skalierbares CMS aufbauen bzw. bestehende Strukturen an die DSA-Vorgaben anpassen. Dazu gehören insbesondere:

- die systematische Identifikation von Risiken, zB durch toxisches Nutzerverhalten, Hassrede oder Verwendung verfassungsfeindlicher Symbole,
- klare Moderationsrichtlinien und Prozesse zur Inhaltskontrolle,
- wirksame interne Beschwerdemechanismen und transparente Entscheidungsdokumentation,
- sowie technisch-organisatorische Maßnahmen, um algorithmische Systeme nachvollziehbar und vertrauenswürdig zu gestalten.

Die regulatorische Entwicklung ist nicht abgeschlossen. Es ist davon auszugehen, dass sich das EU-Digitalrecht weiter ausdifferenzieren und auch auf neue Technologien wie KI-gestützte Moderation, virtuelle Realitäten oder Plattformökonomien aus-

weiten wird. Die Schaffung sicherer, fairer und verantwortungsvoll moderierter Spielräume wird in Zukunft nicht nur ein rechtlicher Imperativ, sondern ein entscheidender Wettbewerbsfaktor für erfolgreiche Gaming-Plattformen sein.

Schnell gelesen ...

- **DSA-Geltungsbereich:** Der DSA reguliert Online-Dienste nach Größe und Funktion, inklusive Gaming-Plattformen und Kommunikationsdienste wie Discord.
- **Compliance-Management-System (CMS):** Games-Anbieter müssen ein CMS implementieren, das interne Prozesse, Richtlinien, Schulungen und fortlaufende Überwachung umfasst.
- **Melde- und Beschwerdeverfahren:** Wichtig sind nutzerfreundliche Systeme zur Meldung illegaler Inhalte (Art. 16 DSA) und zur Anfechtung von Moderationsentscheidungen (Art. 20 DSA).
- **Transparenz und Organisation:** Regelmäßige Transparenzberichte (Art. 15, 42 DSA) und eine angepasste Compliance-Organisation sind erforderlich.
- **VLOPs und Sanktionen:** Sehr große Plattformen haben strengere Pflichten. Verstöße können zu hohen Bußgeldern (bis zu 6% des Jahresumsatzes) führen.



Olaf Wolters

ist Rechtsanwalt bei Nordemann in Berlin.