Beirat beim Digital Services Coordinator

Handreichung zum
Schutz Minderjähriger im Internet
nach dem Digital Services Act (Art. 28 DSA)

1. Schutzziele des Art. 28 Abs. 1 DSA

Art. 28 DSA formuliert grundsätzliche Anforderungen für Anbieter von Online-Plattformen zum Schutz Minderjähriger online. Nach Art. 28 Abs. 1 DSA müssen Anbieter von Online-Plattformen, deren Dienste für Minderjährige grundsätzlich zugänglich sind, geeignete Maßnahmen ergreifen, um drei grundlegende Schutzziele zu erreichen: ein hohes Maß an
1) Privatsphäre, 2) Sicherheit und 3) Schutz von Minderjährigen im Kontext ihres Dienstes oder Produkts. Implizit scheint die Logik von Art. 28 DSA darauf zu fußen, dass Diensteanbieter in der Lage sein müssen, zwischen minderjährigen und erwachsenen Nutzenden zu unterscheiden, um gegenüber Minderjährigen Maßnahmen zu ihrem Schutz, ihrer Sicherheit und Privatsphäre ergreifen zu können.

Diese Schutzziele – Privatsphäre, Sicherheit und Schutz – sind nicht weiter definiert. Erwägungsgrund 71 weist auf das grundlegende Spannungsverhältnis zwischen den Zielen Schutz und Sicherheit auf der einen Seite und Privatsphäre auf der anderen Seite hin, das auch in Art. 28 Abs. 2 DSA (Verbot der Darstellung von personalisierter Werbung gegenüber Minderjährigen) und Art. 28 Abs. 3 DSA (keine Verpflichtung zur Verarbeitung zusätzlicher personenbezogener Daten, um das Alter einer Nutzerin oder eines Nutzers festzustellen) deutlich wird.

Beirat bei der Koordinierungsstelle
für Digitale Dienste

Hausadresse:
c/o Bundesnetzagentur
Tulpenfeld 4
53113 Bonn

Telefon
0228 14-0

Telefax
0228 14-6456

E-Mail
Geschaeftsstelle.BL@BNetzA.DE

Internet
http://www.dsc.bund.de

Erwägungsgrund 71 unterstreicht, dass die Verpflichtungen in Art. 28 DSA nicht zu neuen Anreizen für Online-Plattformen führen sollten, das Alter ihrer Nutzenden zu erfassen, bevor diese ihre Dienste nutzen, und dass insbesondere der Grundsatz der Datenminimierung beachtet werden soll. Damit bleibt unklar, in welchem Verhältnis die in Art. 28 Abs. 1 DSA ausgedrückten Schutzziele zueinanderstehen und wie das inhärente Spannungsverhältnis aufgelöst werden kann. Dieses Spannungsverhältnis drückt sich insbesondere in der Frage aus, ob und wenn ja, für welche Diensteanbieter es notwendig ist, das Alter ihrer Nutzenden zu bestimmen, um den Anforderungen von Art. 28 DSA gerecht zu werden.

Zur Beantwortung dieser Frage ist es hilfreich, dass Erwägungsgrund 71 den Hinweis enthält, dass die Maßnahmen, die Online-Plattformen zum Schutz Minderjähriger treffen müssen, nicht nur *geeignet,* sondern auch *verhältnismäßig* sein sollen. In aktuellen politischen Debatten zum Schutz Minderjähriger online wird häufig angenommen, dass die Altersbestimmung eine notwendige Komponente von Schutzkonzepten ist, ohne die Eignung und Verhältnismäßigkeit dieser Maßnahme zu prüfen. Stattdessen wird die Debatte häufig auf die Frage nach den geeignetsten Methoden zur Altersbestimmung verengt. Insbesondere im Kontext der sich etablierenden Haltung der Europäischen Kommission, dass der Einsatz von Altersbestimmungstechnologien notwendig ist, um Compliance mit Art. 28 DSA und den darin formulierten Schutzzielen zu demonstrieren, muss eine Prüfung ihrer Eignung und Verhältnismäßigkeit ein zentrales Anliegen sein.

Mit Blick auf die **Eignung** von Altersbestimmungstechnologien für den Schutz von Minderjährigen sollte beachtet werden:

- Die Eignung von Technologien, nicht umgangen zu werden. Dabei sollte sowohl geprüft werden, wie leicht ein System zur Altersbestimmung von Minderjährigen umgangen werden kann, als auch das Szenario, dass Erwachsene sich Zugang zu geschützten Räumen für Kinder verschaffen. Grundsätzlich muss angenommen werden, dass jede Form der Altersbestimmung umgangen werden kann.

.

- Ein weiterer relevanter Aspekt ist die Frage, in welchen Kontexten eine Altersbestimmung geeignet ist, um die in Art. 28 DSA ausgeführten Schutzziele zu erreichen: Dienste von Online-Plattformen unterscheiden sich hinsichtlich ihrer Funktionen, Richtlinien und Nutzenden, was zu unterschiedlichen Risikoprofilen führt. Dafür ist eine differenzierte Betrachtung der Risikofaktoren der Dienste nötig, die unter Art. 28 DSA fallen. Die im Kontext von Art. 28 DSA erarbeiteten Guidelines sollten Standards für solche Risikobewertungen beinhalten. Dabei sollte grundsätzlich zwischen den Risikokategorien *content* (Zugang zu entwicklungsbeeinträchtigenden Inhalten), *conduct* (gefährdendes Verhalten Minderjähriger wie cyberbullying, sexting etc.) und *contact* (Interaktionen mit Personen, die Risiken für Minderjährige darstellen können) unterschieden werden.

Mit Blick auf die **Verhältnismäßigkeit** vom Einsatz von Altersbestimmungstechnologien sollten folgende Faktoren beachtet werden:

- Die Auswirkungen von Altersbestimmungstechnologien auf die Grundrechte aller Nutzenden, insbesondere:
    - das Recht auf Privatsphäre,
    - den Schutz personenbezogener Daten,
    - die Freiheit der Meinungsäußerung und die Informationsfreiheit sowie
    - die Rechte des Kindes.

- Die Möglichkeit einer anonymen Internetnutzung ist wichtig und muss erhalten bleiben.

- Um die Verhältnismäßigkeit des Einsatzes von Altersbestimmungstechnologien bestimmen zu können, sollte zudem wissenschaftliche Evidenz zu den realen Risiken und Auswirkungen von Online-Plattformen auf Minderjährige einbezogen werden. Hier sollte beachtet werden, dass die Wechselwirkungen zwischen dem Konsum von digitalen Medien und der Gesundheit und Entwicklung von Minderjährigen umstritten und empirisch besonders schwer zu erforschen ist.

.

Der Ausgleich der in Art. 28 DSA genannten, zueinander in Spannung stehenden Schutzziele sollte nicht einzelnen Anbietern von Online-Plattformen obliegen. Vielmehr müssen die Guidelines klare Richtlinien enthalten, um die spezifischen Risiken eines Dienstes zu bestimmen und, darauf aufbauend, angemessene und wirkungsvolle Schutzmaßnahmen zu definieren.

2. Altersverifikationssysteme

Systeme zur Altersverifikation bzw. Alterseinschätzung dienen dazu, bestimmte Online-Inhalte oder Online-Anwendungen nur Personen einer bestimmten Altersgruppe zugänglich zu machen. Dabei kann es sich einerseits um die Überprüfung eines Mindestalters handeln, um zum Beispiel Minderjährige vor bestimmten jugendgefährdenden Inhalten zu schützen. Andererseits kann auch ein Höchstalter geprüft werden, um beispielsweise einen Kommunikationsraum nur für Kinder oder Jugendliche anzubieten und so Interaktionsrisiken zu minimieren.

Der Einsatz von Systemen zur Altersverifikation bzw. Alterseinschätzung muss einerseits praxistauglich sein und andererseits zugleich die (Schutz-)Rechte von Kindern und Jugendlichen berücksichtigen. Daher sind folgende Punkte wichtig:

- Sowohl der Anwendungsbereich der Systeme im Hinblick auf die zu reduzierenden Risiken der einzelnen Dienste als auch das technische Set-Up der jeweiligen Diensteanbieter sind divers. In der Folge kann es nicht „das eine Altersverifikationssystem“ geben. Vielmehr ist eine Mehrzahl an Systemen zur Altersverifikation bzw. Alterseinschätzung in Kombination mit einer Auswahlmöglichkeit durch die jeweiligen Diensteanbieter zuzulassen.

- Wird ein System zur Altersverifikation bzw. Alterseinschätzung seitens des Diensteanbieters eingesetzt, muss es das jeweilige Schutzziel erreichen können.

.

- Datenschutzrechtliche Aspekte wie beispielsweise der Grundsatz der Datensparsamkeit sind zwingend zu berücksichtigen. Im Hinblick auf die Überprüfung des Alters der Nutzerinnen und Nutzer, insbesondere aber von Kindern bzw. Jugendlichen sind Systeme einzusetzen, bei denen keine personenbezogenen Daten erhoben und verarbeitet werden. Hierdurch würde nicht nur dem Datenschutz an sich weitgehend Rechnung getragen, sondern auch die Vorgabe von Art. 28 Abs. 3 DSA eingehalten, dass Anbieter von Online-Plattformen nicht zur Verarbeitung personenbezogener Daten verpflichtet sind, wenn sie das Alter minderjähriger Nutzender überprüfen.

- Bei der Verwendung von Mini Wallets bzw. digitalen Identitäten darf nur die Information ausgespielt werden, dass ein Nutzer oder eine Nutzerin eine bestimmte Altersgrenze überschritten hat. Dies ist ein datenschutzrechtlich positiv hervorzuhebender Ansatz. Da für die Wallets grundsätzlich ein Ausweisdokument erforderlich ist, muss sich für eine breite Anwendung dieses Verifikationsansatzes perspektivisch der Herausforderung gestellt werden, dass Ausweisdokumente in der Regel erst ab einem bestimmten Alter zugänglich sind.

- Beim Einsatz von Systemen zur Altersverifikation bzw. Alterseinschätzung sind die möglichen Auswirkungen und Konsequenzen für die IT-Sicherheit zu bedenken und zu berücksichtigen. Es gilt, eine Schwächung der IT-Sicherheit zu vermeiden.

- Bereits heute existiert eine Vielzahl von Systemen zur Altersverifikation bzw. Alterseinschätzung. Insofern hat Deutschland durch den Jugendmedienschutz-Staatsvertrag sowie dessen Anwendung durch die FSM und KJM etablierte Kriterien und Best Practices. Diese sollten durch den DSC bzw. die weiteren zuständigen Behörden im Rahmen von Initiativen und Aktivitäten der europäischen Institutionen rund um das Thema „Altersverifikation“ eingebracht werden. Ferner ist wichtig, dass bei Ausschreibungen der Europäischen Kommission die nationalen DSC informiert und eingebunden werden.

.

3. Design- und Default-Maßnahmen

Kinder und Jugendliche sollten in der Lage sein, die Vorteile des Internets zu nutzen, Gemeinschaften aufzubauen und sich auszudrücken. Dabei muss ihre Privatsphäre gewahrt sowie für ihre allgemeine Sicherheit gesorgt sein. Derzeit sind Kinder jedoch auf Online-Plattformen einer großen Reihe von Risiken ausgesetzt mit teils gravierenden Folgen für die minderjährigen Nutzerinnen und Nutzer. Zielgruppengerechtere Design- und Defaulteinstellungen helfen, Risiken zu minimieren, damit sich minderjährige Nutzende möglichst unbeschadet im Internet bewegen können.

Grundlegende Accounteinstellungen

Accounts von Kindern und Jugendlichen sollten standardmäßig besonders datenschutzsensibel und datensparsam ausgestaltet sein, um ihre Privatsphäre zu schützen. Hierzu zählen sowohl die Verwendung von verhaltensbezogenen Daten für Werbe- und Personalisierungszwecke als auch der Schutz vor uneingeschränkter Sichtbarkeit.

- Die Konten sollten grundsätzlich auf ‚privat' gestellt sein und nicht in den Suchmaschinen auftauchen.

- Deaktivierung von Tracking-Mechanismen wie nicht notwendige Cookies, Pixel und Ortungstechniken

- Einschränkung sensibler Funktionen wie die Mikrofon- und Kameranutzung

- Keine Tracking-basierte Werbung gegenüber Kindern und Jugendlichen

- Die Nutzung der Kommunikationsdaten sowie der für sie bestimmten Endgeräte und Software muss streng begrenzt sein.

.

- Einschränkung von Online-Zahlungen bspw. durch Festlegung von Standardausgabelimits für Kinderkonten und standardmäßige Deaktivierung von In-Game-Käufen

Kind- und jugendgerechte Gestaltung

Die Gestaltung von Plattformen und insbesondere Sicherheitsanwendungen müssen auf die Bedürfnisse minderjähriger Nutzender angepasst werden. Vor allem sollten diese niederschwellig, verständlich und nicht verhaltenssteuernd ausgestaltet sein.

- Kinderfreundliche, leicht verständliche Sprache und Oberflächengestaltung der Online-Plattform, insbesondere der Sicherheitsfunktionen

- Meldesysteme
    - Die Meldemöglichkeit muss auch für nicht registrierte Kinder zur Verfügung stehen, wenn der Inhalt für sie zugänglich ist.
    - Die Meldeoption muss mit höchstens zwei Klicks über deutlich gekennzeichnete Links erreichbar sein.
    - Die gemeldeten Inhalte müssen entsprechend den Vorgaben des DSA unverzüglich überprüft werden, wenn erhebliche und schwerwiegende Gefahren bestehen.
    - Bei der Meldung und auf Wunsch wird automatisch ein rechtssicherer Screenshot an die meldende Person übersandt.

- Leicht auffindbare und anwendbare Funktion zur Löschung von eigenen Inhalten und der Kontolöschung im Ganzen

- Verbot des Einsatzes von manipulativen Design-Anwendungen gegenüber minderjährigen Nutzenden wie beispielsweise endloses Scrollen, Autoplay-Funktionen, Push-Benachrichtigungen

.

Kuratieren von Inhalten

Accounts von Kindern und Jugendlichen sollten nicht allein durch Interaktionsraten gesteuert sein, sondern vor allem altersgerechte und differenzierende Inhalte bevorzugen und Wahlmöglichkeiten zulassen. Kinder und Jugendliche müssen vor jugendgefährdenden Inhalten geschützt werden.

- Empfehlungssysteme sollten auf altersgerechte, differenzierende Inhalte sowie inhaltliche Relevanz hin optimiert werden.
    - Engagement-basierte Empfehlungssysteme müssen ausgeschaltet sein.
    - Algorithmen sollten die Qualität und Relevanz von Inhalten in den Vordergrund stellen und die Wahlmöglichkeiten der Nutzenden, durch die sie Präferenzen angeben können.

- Verbot der Ausspielung von Werbung für Produkte und Dienstleistungen, die für Kinder schädlich und ungeeignet sind

Schutz vor bildbasierter digitaler Gewalt bei Accounts von minderjährigen Nutzenden

Kinder und Jugendliche müssen insbesondere auch vor schädlichen Bild- und Videoinhalten geschützt werden, indem diese bspw. unkenntlich gemacht werden. Gleichzeitig sind nutzergenerierte Bild- und Videoinhalte von Kindern und Jugendlichen vor Missbrauch mit möglicherweise lebenslangen Folgen zu schützen.

Folgende Maßnahmen könnten - ohne Anspruch auf Vollständigkeit - diesem Zweck dienlich sein:

- Schutz von eingestellten Bildern durch Screenshot Blocker (z.B. be real) und Kopier- und Deepfakeschutz, bei dem sich die Bilder bei Manipulation verändern; hierdurch kann das Risiko, dass von Kindern und Jugendlichen eingestellte Bilder zweckentfremdet und so ihrer Kontrolle entzogen werden, zumindest verringert werden

.

- Blurren von Privatnachrichten und ggf. auch Inhalten, die pornografische oder gewaltvolle Abbildungen enthalten, ggf. durch Anklicken optional durch Nutzende „entsperrbar“ (Bsp. Bumble oder Moderationstools)

Die Umsetzung technischer Maßnahmen zum Schutz vor bildbasierter digitaler Gewalt muss im Rahmen einer Gesamtfolgenabschätzung technisch wirksam sein, ohne die Sicherheit und Integrität digitaler Kommunikation zu unterminieren.

Anmerkung:

Diese Handreichung wurde verfasst, bevor der Entwurf der Leitlinien zum Schutz Minderjähriger im Internet nach dem Gesetz über digitale Dienste von der EU-Kommission am 13. Mai 2025 veröffentlicht wurde.

Der Beirat beim DSC:

Der Beirat beim Digital Services Coordinator unterstützt als Expertengremium den DSC bei der Wahrnehmung seiner Aufgaben im Rahmen des Digital Services Act (DSA) und wirkt als Bindeglied zu Wissenschaft und Praxis.

Weitere Informationen hierzu:

https://www.dsc.bund.de/DSC/DE/1DSC/Beirat/start.html

Prof. Dr. Henrike Weiden
Vorsitzende des Beirates bei der
Koordinierungsstelle für Digitale Dienste

(Veröffentlicht am 23.05.2025)