Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München
Telefon: +49 (0)89/3176-0
Fax: +49 (0)89/3176-1000
www.microsoft.com/germany

Kontaktpersonen:
- Dr. Guido Brinkel
Leiter Regulierungspolitik /
Director Corporate Affairs
- Rebekka Weiß, LL.M.
Senior Manager Government Affairs

Microsoft Deutschland GmbH
Niederlassung Berlin
Unter den Linden 17
10117 Berlin

guido.brinkel@microsoft.com
rebekka.weiss@microsoft.com

Berlin, Juli 2024

Stellungnahme der Microsoft Deutschland GmbH zum notifizierten Entwurf der Reform des Jugendmedienschutz-Staatsvertrags (JMStV)

I. Einleitung

Die neuen Bestimmungen des Jugendmedienschutzstaatsvertrages (JMStV) in Deutschland zielen darauf ab, spezifische Anforderungen für Anbieter von Betriebssystemen, Apps und Browsern einzuführen. Der Text ist im April bei der EU-Kommission notifiziert worden.

Neben zahlreichen technischen und rechtlichen Fragestellungen hat der JMStV Auswirkungen auf den digitalen Binnenmarkt. Die Anforderungen führen zu einer Fragmentierung innerhalb der EU, da sie deutschlandspezifische Verpflichtungen auferlegen, was den Zielen der EU, einen harmonisierten digitalen Markt in allen Mitgliedsstaaten zu fördern, zuwiderläuft. Der digitale Binnenmarkt wird hierdurch beeinträchtigt.

Der digitale Binnenmarkt der EU soll den freien Waren-, Dienstleistungs- und Kapitalverkehr innerhalb der EU gewährleisten und Bürgern und Unternehmen den Zugang zu und die Ausübung von Online-Aktivitäten ermöglichen. Die Einführung neuer, länderspezifischer Anforderungen behindert diese Harmonisierung und führt zu einem Flickenteppich von Vorschriften, der die Einhaltung der Vorschriften für EU-weit tätige Unternehmen erschwert, Innovationen hemmt und unterschiedliche Verbraucherschutzniveaus auf dem Markt einführt.

Insbesondere im Hinblick auf digitale (und Medien-)Dienste widersprechen solche Bestimmungen den weitergehenden Zielen der EU, das Vertrauen der Verbraucher, ein integratives Wachstum und harmonisierte Regeln und Schutzmaßnahmen für alle zu fördern.

Unsere Stellungnahme nimmt auf wesentliche Umsetzungsherausforderungen in technischer, rechtlicher und praktischer Sicht Bezug. Wir halten eine Überprüfung und Überarbeitung des JMStV für angezeigt, um den Zielstellungen des Jugendschutzes gerecht zu werden und zugleich den europäischen Binnenmarkt zu erhalten.

II. Jugendschutz auf Betriebssystemebene, § 12 JMStV

1. Überblick über die Regulierung auf der Ebene des Betriebssystems

Angesichts der Komplexität der vorgeschlagenen Regelungen erlauben wir uns, die grundsätzliche Regelungslogik des notifizierten Vorschlags, soweit er Betriebssystemanbieter betrifft, zunächst nach unserem Verständnis des Entwurfs zusammenzufassen, um auf dieser Basis zu den einzelnen Aspekten des Vorschlags Stellung nehmen zu können:

Vorhandensein einer Jugendschutzvorrichtung, Aktivierung & Hinweise (§ 12 Abs. 1, 2 JMStV)

- Betriebssysteme müssen grundsätzlich über ein "Jugendschutzvorrichtung" verfügen, das den weiteren Anforderungen des JMStV entspricht (§ 12 Abs. 2 Satz 1 JMStV).
- Das Einrichten, Aktivieren und Deaktivieren muss auf einfache, leicht zugängliche und abgesicherte Weise möglich sein (§ 12 Abs. 2 Satz 1 JMStV).
- Auf die Möglichkeit der Aktivierung ist bei (1.) Erstinbetriebnahme (2.) Erstbereitstellung der Jugendschutzvorrichtung und (3.) Funktionsänderung der Jugendschutzvorrichtung hinzuweisen (§ 12 Abs. 2 Satz 2 JMStV).

Umsetzung der Funktionen bei aktiviertem Gerät und eingestellte Altersangabe (§ 12 Abs. 3 Nr. 1-4 JMStV)

- Die Altersangabe muss in der Jugendschutzvorrichtung eingestellt werden können (§ 12 Abs. 3 Satz 1).
- Wenn eine Altersangabe eingestellt ist, muss das Betriebssystem sicherstellen, dass:
    - Browser, die einen offenen Zugang zum Internet ermöglichen, dürfen nur genutzt werden, wenn sie auf Online-Suchmaschinen zugreifen, die über eine sichere Suchfunktion verfügen oder deren ungesicherter Zugang individuell und abgesichert freigeschaltet wurde (§ 12 Abs. 3 Satz 2 Nr. 1)
    - die Installation von Apps nur über Vertriebsplattformen möglich ist, die die Altersangabe berücksichtigen und ein automatisiertes Bewertungssystem nach Abs. 4 bereitstellen (§ 12 Abs. 3 Satz 2 Nr. 2).
    - nur Apps genutzt werden können, die der Altersangabe entsprechen oder die individuell und abgesichert freigeschaltet wurden (§ 12 Abs. 3 Satz 2 Nr. 3)
    - die Nutzung von Browsern und Apps individuell und abgesichert ausgeschlossen werden kann (§ 12 Abs. 3 Satz 2 Nr. 4)

2. Definition des Begriffs "App" (§ 3 Nr. 9 JMStV) und deren Auswirkungen auf die funktionalen Anforderungen an Jugendschutzvorrichtungen nach § 12 Abs. 3 JMStV

Im Zusammenhang mit den funktionalen Anforderungen an die geforderte Jugendschutzvorrichtung (insbesondere § 12 Abs. 3 Nr. 2 - 4 JMStV sowie § 12 Abs. 4) ist – auch in Bezug auf die überarbeitete notifizierte Fassung - die Definition des Begriffs "App" von entscheidender Bedeutung. Nach § 3 Nr. 9 JMStV *ist* eine "*App eine softwarebasierte Anwendung, die der unmittelbaren Ansteuerung von Angeboten (von Sendungen oder Inhalten von Telemedien) dient*". Die Reichweite dieser Definition bleibt insbesondere bezüglich der Inbezugnahme von „Inhalten von Telemedien" unklar, was zu erheblichen Unsicherheiten und begrifflichen Widersprüchen bei den Funktionsanforderungen an

Jugendschutzvorrichtungen führt. In Abgrenzungen zu „Sendungen" – die den Rundfunkbereich referenzieren – bedürfte es zudem für eine rechtssichere Handhabung einer Definition von Telemedien", die jedoch gesetzlich nicht existiert.

Im allgemeinen Sprachgebrauch ist "App" ein Sammelbegriff für alle Arten von Softwareanwendungen, wobei es keine klare Unterscheidung zwischen "Mobile Apps" und "Desktop Apps" gibt. Auch impliziert der Begriff "App" im allgemeinen Sprachgebrauch nicht, dass eine Internetverbindung erforderlich ist oder dass sie technisch auf Telemedienangeboten basiert oder diese in irgendeiner Weise integriert. Mit anderen Worten: Im allgemeinen Sprachgebrauch hat sich der Begriff "App" als Kurzbezeichnung für alle Arten von Softwareanwendungen etabliert, sowohl im mobilen Umfeld als auch auf anderen Klassen von Endgeräten.

3 Nr. 9 JMStV geht von einem engeren Verständnis von "Apps" aus, wenn er verlangt, dass eine App im Sinne des JMStV nur solche softwarebasierten Anwendungen sein soll, *"die der **unmittelbaren** Ansteuerung einer Sendung oder des Inhalts von Telemedien dient."* Im engsten Sinne könnte dies so verstanden werden, dass nur Mediatheken und Radio-Streaming-Apps ("Steuerung von Rundfunk") sowie Webbrowser ("Steuerung von Telemedien") als "App" im Sinne des JMStV gemeint sind, da nur diese die entsprechende Steuerung als unmittelbare Kernfunktionalität haben. Die Definition selbst enthält keine näheren Erläuterungen, was unter „unmittelbarer Ansteuerung" zu verstehen ist.

Grundsätzlich haben Softwareanwendungen aller Art heute einen funktionalen Zugriff auf Inhalte aus dem Internet. Die (mobilen) Apps der Verkehrsverbünde oder der Deutschen Bahn (die u.a. Live-Informationen über Verspätungen etc. über das Internet beziehen) oder die "On-Leihe"-Anwendung der deutschen Bibliotheken mögen als Beispiele für die nahezu unbegrenzte Reichweite in dieser Hinsicht dienen. Aber auch funktionale Basisanwendungen wie PDF-Reader, Office-Pakete wie Tabellenkalkulationen und Präsentationsanwendungen, die Daten und Informationen aus dem Internet abrufen und einbinden können, haben heute die Möglichkeit, Inhalte aus dem Netz anzusteuern.

Die Frage, was unter "*der unmittelbaren Ansteuerung des Inhalts von Telemedien dienend*" *zu* verstehen ist, bestimmt den gesamten Anwendungsbereich der Anforderungen des § 12 Abs. 3 Nr. 2-4 JMStV. Die Definition darf daher keinen Zweifel an der Reichweite der von ihr erfassten Anwendungen lassen.

Bei einer zu weiten Auslegung des Begriffs "App" werden andernfalls die entsprechenden Anforderungen in § 12 Abs. 3 Nr. 2 - 4 JMStV insbesondere im PC-Bereich große praktische Probleme aufwerfen. Die Verpflichtung zur Verhinderung der Zugänglichkeit von nicht altersbeschränkten Apps nach § 12 Abs. 3 Nr. 3 JMStV würde beispielsweise bei einer weiten Auslegung auch auf systemkritische Anwendungen im PC-Bereich umfassen.

Wir empfehlen daher eine Klarstellung der Definition bzw. Ausführungen im Begründungsteil des JMStV, wie der Begriff der „unmittelbaren Ansteuerung" zu verstehen ist und welche Inhalte über den Begriff der „Telemedien" erfasst sein sollen. Dies ist einerseits vor dem Hintergrund umfassender bereits bestehender Regelungen aus dem Digitale Dienste Gesetz als auch im Bereich des Rundfunks erforderlich. Und andererseits ist eine Klarstellung auch vor dem Hintergrund relevant, dass durch das Außerkrafttreten des Telemediengesetzes (TMG) einige Begriffsunschärfen bestehen, die auch durch das neue Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (TDDDG) bisher nicht vollständig aufzulösen sind.

3. Funktionale Anforderungen an Betriebssysteme nach Aktivierung der Jugendschutzvorrichtung, § 12 JMStV

a) Sichere Suche und Browser, § 12 Abs. 3 Satz 2 Nr. 1 JMStV

12 Abs. 3 Satz 2 Nr. 1 JMStV schreibt vor, dass bei aktivierter Jugendschutzvorrichtung "*bei Browsern, die einen offenen Zugang zum Internet eröffnen, eine Nutzung nur möglich ist, sofern sie Online-Suchmaschinen ansteuern, die über eine gesicherte Suchfunktion verfügen oder deren ungesicherter Zugang individuell und in abgesicherter Weise freigeschaltet wurde*".

Diese Verpflichtung wirft Fragen im Hinblick auf die technische Durchführbarkeit, den Umfang der rechtlichen Anforderungen und die beabsichtigte praktische Schutzwirkung auf. Der vorgeschlagene Mechanismus will in der nun notifizierten Fassung den Anbieter des Betriebssystems bei aktivierter Jugendschutzvorrichtung verpflichten, den Zugang zu Suchmaschinen nur zuzulassen, soweit diese eine sichere Suchfunktion anbieten. Suchmaschinen ohne eine solche Funktion dürften demnach bei aktivierter Jugendschutzvorrichtung nicht angesteuert werden.

Allerdings wird weder im (Entwurf) des Staatsvertrags noch in anderen Gesetzen legaldefiniert, was überhaupt als "gesicherte Suchfunktion" in diesem rechtlichen Kontext gilt. Dies bedeutet, dass die Anbieter von Betriebssystemen das Risiko tragen würden, zu entscheiden, ob eine Suchmaschine einen Mechanismus bereitstellt, der nach dieser Regelung rechtlich ausreichend wäre.

Die eigentliche rechtliche Verpflichtung dieser Bestimmung besteht im Umkehrschluss zum Regulierungsbefehl des § 12 Abs. 3 S. 2 Nr. 1 darin, den Zugang zu allen Suchmaschinen zu unterbinden, die keine „gesicherte Suchfunktion" bieten, sobald die Jugendschutzvorrichtung auf einem bestimmten Gerät aktiviert wird. Das bedeutet, dass der Anbieter des Betriebssystems dafür sorgen müsste, dass - über alle auf einem Gerät verfügbaren Browser hinweg - eine bestimmte Gruppe von Suchmaschinen (basierend auf den fehlenden Kriterien, ob sie eine „gesicherte Suchfunktion" bieten oder nicht) nicht mehr verfügbar ist.

Dies würde ein Blacklist-Konzept für eine breite Palette von Suchmaschinen, einschließlich Metasuchen[1], erfordern. Die Vorschrift würde (im Falle einer aktivierten Jugendschutzvorrichtung) von Betriebssystemanbietern aller Art verlangen, den Zugang zu einer Reihe von Suchmaschinen über alle Browser hinweg ausschließlich für den deutschen Markt zu sperren, sobald die Vorrichtung auf einem Gerät aktiviert, wurde. Dies widerspricht dem einheitlichen digitalen Binnenmarkt und bedürfte aus rechtsstaatlicher Sicht jedenfalls weiterer prozessualer Absicherung dahingehend, dass eine solche Blacklist von der KJM auf Basis transparenter Kriterien zentral erstellt und autorisiert werden müsste.

[1] Metasuchen sind Suchmaschinen, die die Ergebnisse verschiedener Suchmaschinen bündeln und anzeigen. Mit Metasuchen können gleichzeitig verschiedene Suchmaschinen durchsucht und die Ergebnisse (mit Referenzangaben) indexiert werden.

b) Verhinderung der Installation und Ausführung von Programmen außerhalb der "systemeigenen Vertriebsplattform" (§ 12 Abs. 3 Nr. 2 und 3)

12 Abs. 3 Nr. 2 verlangt, dass das Betriebssystem bei aktivierter *Jugendschutzvorrichtung* sicherstellt, "*dass die Installation von Apps nur über Vertriebsplattformen möglich ist, die die Altersangabe berücksichtigen und ein automatisiertes Bewertungssystem nach Absatz 4 vorhalten.*"

Die Vorschrift lässt – auch in ihrer nun notifizierten Fassung - zwei Interpretationen bzgl. ihres Verfügungscharakters zu:

1. Generell soll bei aktivierter Jugendschutzvorrichtung die Installation von Apps ausschließlich über Vertriebsplattformen (App-Stores) möglich sein, die zudem die qualifizierten Anforderungen des § 12 Abs. 2 S. 2 Nr. 2 JMStV erfüllen müssen.

   oder abweichend…

2. Soweit im Falle einer aktivierten Jugendschutzvorrichtung die Installation von Apps über Vertriebsplattformen, also App-Stores, erfolgt müssen diese den qualifizierten Anforderungen des § 12 Abs. 2 S. Nr. 2 JMStV entsprechen.

Wir regen an, § 12 Abs. 2, S. 2 Nr. 2 JMStV wie folgt im Sinne der 2. Variante zu präzisieren:

> *„soweit die Installation von Apps über eine Vertriebsplattform erfolgt, diese die Altersstufe berücksichtigen muss."*

Diese Präzisierung würde erheblich dazu beitragen, die Folgen für das PC-Ökosystem, in dem App-Stores nicht den primären Installationsweg für Software bilden, abzumildern. Durch die zur Zeit vorgeschlagene Regelung sind, wie nachfolgend detailliert dargelegt wird, andernfalls schwerwiegende Folgen durch die Anwendung der Vorgaben zu erwarten.

aa) Beschaffungskanäle für Softwareanwendungen im PC-Ökosystem – Installation abseits von App-Stores als Primärinstallationsweg

Die Bestimmung(en) wurde(n) offenbar primär mit Blick auf mobile Betriebssysteme eingefügt, bei denen der "App-Store" typischerweise der zentralen oder sogar einzige vorgesehene Installationspfad für Software ist. In diesen Ökosystemen sind Altersfreigaben in Apps die Regel, weshalb für Installationen außerhalb des App-Stores häufig der Begriff "Sideloading" verwendet wird. Dabei wird jedoch übersehen, dass bei anderen Endgerätekategorien, insbesondere bei PC´s, eine "native" Distributionsplattform, also ein eigener App-Store, nicht die Regel ist oder für einzelne Betriebssysteme, insbesondere Linux, gar nicht existiert. Gleiches gilt in der Folge für Alterskennzeichnungen von Software, die im PC-Bereich für frei aus dem Internet oder via Datenträger installierbare Programme praktisch nicht vorhanden sind. Die Nutzererfahrung im PC-Bereich umfasst daher stets auch die Erwartungshaltung, zusätzliche Anwendungen frei aus dem Internet beziehen zu können.

Der nun notifizierte Vorschlag wirft, wie schon die Vorgängerversionen des Vorschlags, die grundsätzliche Frage auf, wie Betriebssysteme, die nicht über eine eigene Vertriebsplattform verfügen oder bei denen diese nicht der Hauptbeschaffungskanal für Software ist, mit der entsprechenden Anforderung umgehen sollen. Im Falle von Microsoft Windows gibt es zwar einen "App-Store" in Form des Microsoft Stores, aber Windows ist traditionell als offenes Betriebssystem konzipiert, das die Installation von Software aus dem Internet über Browser unterstützt.

Anders als im Bereich der mobilen Betriebssysteme sind große Teile der Softwarelandschaft im PC-Bereich nur als freie Installationen (entweder über das Internet oder über Datenträger) verfügbar. Dies gilt für alle Formen von Software und damit für die gesamte Palette jugendschutzneutraler Angebote (z. B. PDF-Reader, Bildbearbeitungsprogramme, Systemprogramme etc.), aber auch für kinder- und jugendspezifische Angebote wie die Desktop-Versionen von Lernplattformen[2] oder Übersetzungsangebote. Letztlich verhält sich das PC-Ökosystem in Bezug auf die Bezugswege für Software reziprok zu mobilen Betriebssystemen. Während bei diesen Installationen abseits des App-Stores per Design die Ausnahme bilden (deshalb häufig als „sideloading" bezeichnet) bildet die freie Installation abseits von App-Stores im PC-Ökosystem den Hauptinstallationsweg für Software.

bb) Overblocking-Effekt im PC-Ökosystem

Im PC-Bereich führt die Vorschrift des § 12 Abs. 3 Nr. 2 daher faktisch bei aktivierter Jugendschutzfunktion zu einer fast vollständigen Sperrung des Hauptinstallationsweges für Software bzw. jedenfalls zu einem massiven overblocking durch die Jugendschutzvorrichtung, weil alle Installationskanäle abseits der Vertriebsplattformen per default zu sperren wären. Dies würde mit an Sicherheit grenzender Wahrscheinlichkeit zu grundsätzlichen Akzeptanzproblemen führen bzw. unweigerlich dazu, dass Eltern diese Blockade im Sinne des § 12 Abs. 3 Nr. 2 JMStV individuell aufheben oder die Jugendschutzvorrichtung gänzlich wieder deaktivieren.

Offenbar bestehen zu dieser Problematik auf Ebene der Rundfunkkommission Bedenken, dass eine Beschränkung der Vorgabe auf Vertriebsplattformen geeignet ist, das gesamte Schutzsystem in Frage zu stellen, da die Berücksichtigung von Altersangaben auf Apps aus Vertriebsplattformen beschränkt wäre, während parallel aus dem Internet jegliche Software heruntergeladen und installiert werden könnte.

Während diese Einschätzung formal-objektiv richtig ist, möchten wir dringend darauf hinweisen, dass der im Wesentlichen problematische, akzeptanzuntergrabende Overblocking-Effekt dadurch ausgelöst wird, dass von der damit bewirkten Installations- und – über § 13 Abs. 3 Nr. 3 JMStV – Ausführungsblockade auch sämtliche aus Jugendschutzperspektive völlig unproblematischen Anwendungen und sogar spezifische Angebote für Kinder und Jugendliche erfasst werden.

In der Praxis würden Eltern, welche die Jugendschutzlösung aktivieren – völlig unabhängig von der festgelegten Altersstufe – damit konfrontiert, dass die Installation und Ausführung *sämtlicher* Software-Anwendungen blockiert wäre und jeweils erst individuell freigegeben werden müsste. Ein solcher Mechanismus widerspricht grundsätzlich der Erwartungshaltung von Eltern, die Jugendschutzlösungen in der Annahme installieren, spezifisch

[2] Beispiele hierfür sind die Desktop-Versionen von *Sofatutor* und *Simpleclub*. Beide Anbieter bieten Desktop-Versionen, aber keine zusätzlichen Apps im Microsoft Store an.

Jugendschutzrelevante Anwendungen besser kontrollieren zu können, nicht aber eine Einzelfallentscheidung zu jeder einzelnen jugendschutzrechtlich agnostischen Softwareanwendung, seien es Browser, Bildbearbeitungsprogramme, Übersetzungsprogramme, PDF-Reader etc treffen zu müssen.

cc) Sperrung der Ausführung von Apps, die nicht altersbeschränkt sind, § 12 Abs. 3 Nr. 3 JMStV

§ 12 Abs. 3 Nr. 3 JMStV sieht vor, dass "*nur solche Apps nutzbar sind, die der Altersangabe entsprechen oder die individuell und in abgesicherter Weise freigeschaltet wurden.*"
Während § 12 Abs. 3 Nr. 2 darauf abzielt, die *Installation* von Apps zu verhindern, die nicht einer festgelegten Altersangabe entsprechen, befasst sich § 12 Abs. 3 Nr. 3 offenbar mit der Situation von (vor-)installierten Anwendungen und dem Umgang mit diesen, sobald die Jugendschutzvorrichtung aktiviert ist. Die Probleme, die sich aus diesem Ansatz ergeben, sind ähnlich wie die oben unter § 12 Abs. 3 Nr. 2 skizzierten:

So verständlich der Regelungsansatz auf den ersten Blick erscheint, so problematisch sind seine Folgen in der Praxis, insbesondere im Hinblick auf die geforderte Sperrung von Apps, die keine Altersbeschränkung haben. Denn zu dieser Gruppe - zumindest nach dem Wortlaut der Vorschrift - würden auch zahlreiche Anwendungen (d.h. "Apps") gehören, die für die tägliche Nutzung des PCs unerlässlich oder sogar systemkritisch und zugleich aus Sicht des Jugendmedienschutzes völlig unproblematisch sind.

Dazu gehören viele Anwendungen wie PDF-Reader und andere Office-Anwendungen, aber auch Systemprogramme wie der jeweilige (native) App-Store (der selbst auch eine Anwendung im Sinne von § 3 Nr. 9 JMStV ist) sowie Systemverwaltungsanwendungen (z. B. die Systemuhr, die die aktuelle Systemzeit über das Internet bezieht). Diese Anwendungen sind häufig vom jeweiligen Hardwarehersteller vorinstalliert und haben ebenfalls Zugang zum Internet. Hier zeigt sich das bereits erwähnte Problem der fehlenden oder nicht hinreichend bestimmten Abgrenzung des Begriffs "App" durch § 3 Nr. 9 JMStV.

Wenn ein solches Programm auf dem Gerät installiert ist und die Eltern nun die Kindersicherung aktivieren würden, wäre die Nutzung solcher Anwendungen standardmäßig verhindert und müsste von den Eltern nach § 12 Abs. 3 Nr. 3 JMStV individuell genehmigt werden. 3 JMStV. Bei bestimmten Systemanwendungen würde die Sperrung sogar zu einer teilweisen oder vollständigen Funktionsunfähigkeit des Endgerätes führen.

Dies entspricht nicht der grundsätzlichen Erwartungshaltung von Eltern bei der Nutzung einer Lösung für den Jugendschutz. Eltern erwarten nicht die Sperrung von jugendschutzrechtlich völlig unproblematischen Programmen. In der Logik des § 12 Abs. 3 Nr. 3 JMStV hätte die Aktivierung der Jugendschutzeinrichtung zur Folge, dass ein Großteil wichtiger Funktionalitäten eines PCs unmittelbar unterbunden würde, denn die Logik des § 12 Abs. 3 Nr. 3 JMStV kehrt das bisherige praktische Regel-Ausnahme-Verhältnis um: Unter den Softwareprogrammen, die nicht altersbeschränkt sind, sind jugendschutzrechtlich problematische Angebote die Ausnahme.

Da die absolute Mehrheit der nicht altersbeschränkten Programme jugendschutzrechtlich unproblematisch ist, schießt die in § 12 Abs. 3 Nr. 3 JMStV vorgenommene Sperrung weit über das Ziel hinaus, was die Akzeptanz der Lösung untergräbt.

Wir regen daher dringend an, die Regelungslogik des § 12 Abs. 3 Nr. 3 JMStV im Hinblick auf nicht altersgekennzeichnete Apps grundlegend zu überdenken - insbesondere, weil solche lokalen Regelungen und Vorgaben dem europäischen digitalen Binnenmarkt schaden. Ziel muss es sein, den Eltern ein Werkzeug an die Hand zu geben, mit dem sie die Anwendungen auf dem Gerät oder Nutzerkonto des Kindes aktiv steuern können. Dies bedeutet nicht, dass alle Anwendungen, die nicht standardmäßig mit einer Altersbeschränkung versehen sind, bei Aktivierung der elterlichen Kontrolle blockiert werden müssen. Vielmehr sollte die Kindersicherung den Eltern die Möglichkeit geben, Apps auf klare Weise zu aktivieren/deaktivieren oder einzuschränken und, sofern ein eigener Distributionsstore vorhanden ist, sicherzustellen, dass nur altersgerechte Apps für Kinderkonten angeboten werden.

dd) Wettbewerbspolitische Fragestellungen im Kontext des EU Digital Markets Act

Wie bereits beschrieben, kommt § 12 Abs. 3 Nr. 2 JMStV einem Verbot der Installation von Softwarte abseits von App-Stores bei aktivierter Jugendschutzeinrichtung gleich. Dieses Verbot würde sich nicht nur auf jugendschutzrechtlich problematische Inhalte beziehen, sondern auf alle Anwendungen, die nicht mit einer Altersfreigabe versehen sind. Darunter fallen auch Anwendungen, die aus Jugendschutzsicht völlig unproblematisch sind. Die Vorschrift führt damit zu einem Overblocking von Anwendungen, die nicht jugendschutzrelevant sind.

Aus diesem Grund muss § 12 Abs. 3 Nr. 2 JMStV auch im Zusammenhang mit dem Digital Markets Act (DMA) gesehen und überprüft werden. Unter wettbewerbspolitischen Gesichtspunkten setzt der DMA die Möglichkeit durch, über verschiedene Kanäle Software (und Apps) zu beziehen. Art. 6 Nr. 4 der endgültigen Fassung des JMStV lautet entsprechend:

> *Der Torwächter gestattet es und ermöglicht es technisch, Software- Anwendungen Dritter und von Dritten betriebene Geschäfte für Software-Anwendungen, die sein Betriebssystem nutzen oder mit diesem interoperieren, zu installieren und effektiv zu nutzen und auf die Software-Anwendungen bzw. Geschäfte für Software-Anwendungen auf anderem Wege als über die betreffenden zentralen Plattformdienste des Torwächters zuzugreifen."*

Die Verhinderung der Installation von Software - unabhängig von ihrer Jugendschutzrelevanz im Einzelfall - wirft für die vom DMA adressierten Anbieter daher wettbewerbspolitische und europarechtliche Fragen auf und sollte mit Blick auf den Digital Markets Act auf ihre Vereinbarkeit mit dem Binnenmarkt geprüft werden.

c) Alterskennzeichnung durch anerkanntes Bewertungssystem, § 12 Abs. 4 JMStV

12 Abs. 4 JMStV fordert weiterhin *"Bei systemeigenen Vertriebsplattformen für Apps ist sicherzustellen, dass Apps mit einer Altersangabe durch ein von der KJM anerkanntes automatisiertes Bewertungssystem einer anerkannten Einrichtung der freiwilligen Selbstkontrolle versehen werden, die vom Betriebssystem ausgelesen werden kann."*[3]

[3] Wir weisen zunächst darauf hin, dass die offizielle Kommissions-Übersetzung des § 12 Abs. 4 JMStV im Rahmen der Notifizierung die deutsche Fassung nicht korrekt wiedergibt. 12 (4) in der deutschen Originalfassung verlangt, dass *alle* Apps über ein anerkanntes System eine Alterseinstufung erhalten müssen.

Die Vorschrift fordert die Bereitstellung eines von der KJM anerkannten automatisierten Bewertungssystems durch eine anerkannte Selbstkontrolle. Auf Basis des bisher geführten Dialogs gehen wir davon aus, dass die Länder ergänzend zu den bestehenden Regelungen im JuSchG hiermit **einen rechtlichen Bezugsrahmen für das erfolgreich etablierte System IARC (International Age Rating Coalition)[4] im JMStV schaffen wollen. Microsoft setzt IARC sowohl im Microsoft Store als auch im X-Box Store ein und gibt App-Entwicklern zudem entsprechende Hinweise für die Altersklassifizierung via IARC.[5]** IARC hat sich als global standardisierte Lösung am Markt etabliert und wird lokal in Deutschland von der USK als anerkannte Selbstkontrolle verwaltet.[6]

Der Entwurf sieht insoweit eine formelle Anerkennung durch die KJM vor. Dies würde - mangels Vorliegens einer solchen Anerkennung - bedeuten, dass IARC momentan nicht den Anforderungen des § 12 Abs. 4 JMStV entspricht, sondern erst den Anerkennungsprozess durchlaufen muss. Aus dem Entwurf wird nicht klar, weshalb die Länder eine formale Anerkennung der KJM für notwendig erachten. Das Beispiel IARC als international standardisierter Ansatz mit lokaler Verankerung via USK zeigt gerade, dass ein Marktversagen nicht vorliegt. IARC wird ständig weiterentwickelt und hat sich in den vergangenen Jahren als hinreichend flexibel erwiesen, um auf Marktentwicklungen zu reagieren. **Wir regen an, die Anforderung einer formalen Anerkennung durch die KJM zu überdenken und stattdessen die Rolle der anerkannten Selbstkontrolleinrichtungen an dieser Stelle zu stärken.**

Eine Anerkennungspflicht der KJM würde im Übrigen, auch wenn IARC grundsätzlich als Bewertungssystem im Sinne des § 12 Abs. 4 JMStV verstanden wird, nach Inkrafttreten des JMStV einen rechtlichen Schwebezustand auslösen, da ein Großteil der Verpflichtungen der §§ 12 ff. JMStV hierauf aufsetzt.

III. Anwendungen mit eigener Jugendschutzlösung, § 12a JMStV

1. Bereitstellen von Anwendungen mit eigener Jugendschutzlösung, § 12a Abs. 1 JMStV

12a JMStV enthält besondere, ergänzende Regelungen für Anbieter von Anwendungen, die ein anerkanntes Jugendschutzprogramm nach § 11 Abs. 2 JMStV (nicht zu verwechseln mit der jetzt eingeführten gesonderten Verpflichtung für Betriebssystemanbieter!) oder ein geeignetes technisches Mittel nach § 5 Abs. 3 Satz 1 JMStV implementiert haben. Nach § 12a Abs. 1 JMStV sind solche Anwendungen "abweichend von § 12 Abs. 3 Nr. 3 JMStV zur Verfügung zu stellen."

Diese Gegenausnahme wirft Fragen nach dem normativen Zusammenspiel zwischen den anerkannten Jugendschutzprogrammen" auf App-Ebene und den Alterseinstufungen des Jugendschutzsystems auf Betriebssystemebene auf. Betrachtet man das beabsichtigte Zusammenspiel zwischen Apps, die ein anerkanntes Programm anbieten, wäre es konsequent, den Anbietern solcher Anwendungen zu erlauben, ihre Anwendungen mit der Stufe "ohne Altersbeschränkung" zu kennzeichnen. Damit wären sie automatisch in den Stores verfügbar, was dem Regelungszweck des § 12a Abs. 1 JMStV entspräche.

[4] IARC ratings for mobile and digitally delivered games from International Age Rating Coalition (globalratings.com)
[5] Altersfreigaben für MSI- und EXE-Apps - Windows apps | Microsoft Learn
[6] Spiele und Apps im IARC-System - Unterhaltungssoftware Selbstkontrolle (usk.de)

Andernfalls würde § 12a JMStV bedeuten, dass die Betreiber von App-Stores eine völlig neue Kennzeichnungslogik außerhalb der bereits (global) implementierten Alterskennzeichnungen implementieren müssten. Dies müsste durch die Einführung eines zusätzlichen technischen Feldes parallel zur eigentlichen Alterskennzeichnung geschehen, dass das Vorliegen einer "eigenen Schutzlösung" signalisiert, ohne dass dies einen technischen Unterschied zu einer Kennzeichnung auf der Ebene "ohne Altersbeschränkung" im Hinblick auf § 12a Abs. 1 JMStV macht.

2. Auslesen der Altersangaben des Jugendschutzgerätes, § 12a Abs. 2 JMStV

12a Abs. 2 JMStV führt eine (zusammenhängende) Verpflichtung sowohl für Betriebssystemanbieter als auch für Anwendungsanbieter ein. Die Vorschrift verpflichtet Betriebssystemanbieter implizit, **eine externe "Altersschnittstelle" zu unterhalten**, indem sie verlangt, dass die Altersinformationen im Betriebssystem auslesbar sein müssen. Anwendungsanbieter mit einer eigenen Schutzlösung sind verpflichtet, diese Altersinformationen auszulesen und entsprechende Angebote nur entlang dieser Altersstufe "auszuspielen", **unabhängig davon, ob sie ihre Anwendung auf einer nativen Vertriebsplattform vertreiben oder nicht.**

Zunächst einmal ist festzustellen, dass eine solche externe "Altersschnittstelle" zwischen Betriebssystem und App-Anbietern noch nicht existiert. Das bedeutet, dass es auch keine technische Standardisierung hierfür gibt. Dies wäre aber Voraussetzung für ein Zusammenspiel zwischen den Betriebssystemanbietern und den Apps zum Auslesen der Altersinformation.

Zur Verdeutlichung: Aus technischer Sicht handelt es sich um eine andere Situation als die bereits heute in App-Stores implementierten Altersklassifizierungen und die darauf basierenden Kontrollmechanismen für Eltern. Bei den etablierten Jugendschutzlösungen erfolgt der entsprechende Abgleich durch den Betreiber des Stores selbst (das ist in der Regel der Betriebssystemanbieter). Daher ist hier keine externe Schnittstelle notwendig, da der notwendige Abgleich durch Anbieter des App-Stores durchgeführt wird. **Der jeweilige App-Anbieter muss also bei den bestehenden Lösungen nicht auf die Altersinformationen des Betriebssystems selbst zugreifen bzw. - in der Terminologie des Entwurfs - diese Informationen nicht "lesen"**.

§ 12a Abs. 2 JMStV fordert die Einführung einer auslesbaren Altersangabe fordert. Damit bestünde die Möglichkeit, über diese Altersschnittstelle das Alter des jeweiligen Gerätenutzers zu ermitteln. Aus datenschutzrechtlicher Sicht, aber auch aus Sicht des Jugendschutzes und der IT-Sicherheit halten wir dies für problematisch.

Es bleibt unklar, was der Entwurf des JMStV technisch genau meint, wenn er die Möglichkeit des Auslesens fordert. Die von den Eltern im Gerät gespeicherten Informationen müssten wohl mindestens auf dem jeweiligen Endgerät für alle Apps zugänglich gemacht werden. Angreifer könnten über eine solche Schnittstelle z.B. gezielt Endgeräte von Kindern oder Jugendlichen identifizieren (z.B. durch Drive-by-Infektionen), um auf Basis dieser Informationen Social-Hacking-Angriffe durchzuführen. **Insbesondere aus Sicht der IT-Sicherheit ist es daher inakzeptabel, solch sensible Informationen über eine von außen lesbare Schnittstelle zur Verfügung zu stellen.**

Darüber hinaus wirft § 12a JMStV die Frage auf, wie ein Anwendungsanbieter mit den bereitgestellten Informationen konkret umgehen soll. Technische Schutzmaßnahmen auf der Anwendungsebene werden in der Regel auch über account- oder profilbasierte Ansätze umgesetzt. Eine Videostreaming-App bietet beispielsweise die Möglichkeit, für

einzelne Familienmitglieder unter einem Account unterschiedliche Profile mit jeweils unterschiedlichen Alterseinstellungen einzurichten. Unabhängig davon, auf welchem Gerät das Konto genutzt wird, kann der Nutzer weiterhin zwischen den in der Anwendung gespeicherten Profilen wählen, wobei die Profile für Erwachsene in der App durch ein Passwort oder eine PIN vor dem unbefugten Zugriff durch Minderjährige geschützt sind.

In diesen Konstellationen verlangt § 12a JMStV nun von den Anbietern der entsprechenden Videostreaming-Anwendung, die gesamte Anwendung auf die betriebssystemeigene Altersstufe umzuschalten, je nach Betriebssystem des gerade genutzten Endgerätes. Das heißt, der Anbieter der Anwendung wird faktisch gezwungen, seine eigene profilbasierte Lösung zu unterdrücken und das vom Betriebssystem vorgegebene Alter der Anwendung durchzusetzen. **Konkret hätte § 12a Abs. 2 JMStV in dem oben beschriebenen Beispiel zur Folge, dass Erwachsenenprofile, auch wenn sie passwort- oder PIN-gesichert sind, in der App unterdrückt werden müssten. Es ist nicht ersichtlich, welcher ordnungspolitische Zweck damit verfolgt wird, da dies dazu führen wird, dass entsprechende proprietäre Lösungen auf der Anwendungsebene unterlaufen werden.** Ein solches Durchgreifen wird auch nicht den Erwartungen der Eltern entsprechen, wenn sie bewusst entsprechende Profile für ihre Kinder in der jeweiligen App angelegt haben.

Insgesamt empfehlen wir daher dringend, die gesamte Regelungsstruktur des § 12a Abs. 2 JMStV zu überdenken. Die sich aus der Bereitstellung ergebende Notwendigkeit der Einführung einer Altersschnittstelle gegenüber App-Anbietern und die damit verbundenen Missbrauchsrisiken stehen in keinem Verhältnis zu den (erhofften) Vorteilen der angeordneten Durchsetzungswirkung der Altersangaben, deren Umsetzung diese Schnittstelle ausschließlich dienen würde. Insbesondere aus der Sicht der Eltern erscheint der vorgesehene Mechanismus eher kontraproduktiv und damit in der vorgesehenen Gesamtstruktur entbehrlich. EU-weit finden gerade umfangreiche Diskussionen über geeignete Mechanismen zur Überprüfung und Weitergabe von Altersangaben statt, u.a. im Rahmen einer von der Europäischen Kommission geleiteten Arbeitsgruppe. Die Entwicklung von Maßnahmen im Zusammenhang mit der Erhebung und Weitergabe von Altersangaben im JMStV birgt die Gefahr, dass die EU-weite Harmonisierung untergraben und diese wichtige Arbeit vorweggenommen wird.

———