



# Sektoruntersuchung – Messenger- und Video-Dienste

## Zusammenfassung

### *Leitfrage der Untersuchung*

Messenger- und Video-Dienste sind für viele Menschen inzwischen ein unverzichtbarer Teil der alltäglichen Kommunikation geworden. Die Verbraucherinnen und Verbraucher können auf verschiedenen Endgeräten Text- und Sprachnachrichten sowie Dateien austauschen und (per Video) telefonieren und alle diese Funktionen individuell einsetzen und kombinieren. Lange bewährte Kommunikationsarten erscheinen somit in einem modernen Gewand. Der **Wunsch nach Individualität oder einer maßgeschneiderten Lösung** für die eigenen Bedürfnisse schlägt sich bei Messenger- und Video-Diensten in einer großen **Vielfalt an Geschäftsmodellen und Anwendungen** nieder. Wie das Bundeskartellamt im Zwischenbericht zu dieser Sektoruntersuchung bereits ausgeführt hat, sind die Funktionen, die Angebote und die wirtschaftliche Bedeutung der Messenger- und Video-Dienste sehr verschieden. Neben den in der Öffentlichkeit besonders bekannten Diensten besteht eine große Bandbreite an Branchenteilnehmenden, welche von internationalen, konzernbetriebenen Diensten mit vielen Millionen Nutzerinnen und Nutzern, hohen Umsätzen und eigenen digitalen Ökosystemen<sup>1</sup> mit starken Positionen auf benachbarten Märkten über nationale

---

<sup>1</sup> Mit dem Begriff "digitales Ökosystem" wird ein Bündel einer Vielzahl an Diensten eines Konzerns mit Wechselwirkungen untereinander bezeichnet, vgl. *Bundeskartellamt*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses zum Digital Markets Act, 25. April 2022, abrufbar unter: [https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59\\_Stellungnahme-Mundt-data.pdf](https://www.bundestag.de/resource/blob/891308/f13edcf322cc218da602e6dc4b58391b/ADrs-20-9-59_Stellungnahme-Mundt-data.pdf) sowie *Bundeskartellamt*, The Evolving Concept of Market Power in the Digital Economy – Note by Germany, abrufbar unter: [https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions\\_Hintergrundpapiere/OECD\\_2022\\_Competition\\_Committee\\_Concept\\_Market\\_Power\\_Digital\\_Economy.pdf?\\_\\_blob=publicationFile&v=2](https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/OECD_2022_Competition_Committee_Concept_Market_Power_Digital_Economy.pdf?__blob=publicationFile&v=2). Siehe z. B. auch *Fletcher*, Digital competition policy: Are ecosystems different?, Note for the OECD Hearing on Competition Economics of Digital Ecosystems, abrufbar unter: [https://one.oecd.org/document/DAF/COMP/WD\(2020\)96/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2020)96/en/pdf). In der Informationstechnik wird mit dem Begriff Ökosystem eine Soft- und Hardware-Architektur bezeichnet, welche auf jeweils ganz eigenen Geräten, Systemen und Zugangsvoraussetzungen beruht und damit entsprechendes Zubehör voraussetzt und hervorbringt, vgl. *Wikipedia*, abrufbar unter: <https://de.wikipedia.org/wiki/%C3%96kosystem>.

oder auf deutschsprachige Regionen konzentrierte Dienste oder Dienste mit besonderen Geschäftsschwerpunkten bis hin zu Open Source-Diensten und freien Anwendungen ohne Gewinnerzielungsabsicht reicht. Es handelt sich um eine weltweit agierende Branche, die nicht nur auf Seiten der größeren Teilnehmenden technologische und digitale Entwicklungen und Innovationen hervorbringt. Konkurrierende Dienste zeichnen sich durch innovative Geschäftsmodelle und Spezialisierungen auf Basis besonderer Services und Funktionen aus. Nicht nur auf Seiten der freien Systeme und Anwendungen gibt es viel Expertise und Engagement in Sachen Unabhängigkeit und Schutz der persönlichen Daten der Nutzerinnen und Nutzer. Allerdings legt die Marktverfassung den Schluss nahe, dass dieses Potential bisher nicht ausgeschöpft, nicht flächendeckend verteilt und nicht so zugunsten eines hohen Datenschutzniveaus eingesetzt wird, wie es möglich wäre. Damit sind neue **verbraucherrechtliche Fragestellungen** aufgekommen. Die Verbraucherinnen und Verbraucher selbst scheinen diese verbraucherrechtlichen Aspekte gegenüber anderen Kriterien bei der Auswahl ihres Messenger- und Video-Dienstes jedoch bisher hintenanzustellen. Daher steht im Zentrum dieses Abschlussberichts zur Sektoruntersuchung Messenger- und Video-Dienste die Leitfrage, wie **Datenschutz als Wettbewerbsparameter** vorangebracht werden kann, um marktweit bei Messenger- und Video-Diensten ein höheres Datenschutzniveau zu erreichen. Welche Anreize und Maßnahmen sind notwendig, damit die Verbraucherinnen und Verbraucher ihren Messenger- und Video-Dienst auch nach der Datenschutzfreundlichkeit auswählen? Und wie können die anbietenden Messenger- und Video-Dienste bewegt werden, Datenschutzfreundlichkeit vermehrt als Differenzierungsmerkmal einzusetzen und die Verbraucherinnen und Verbraucher besser darüber zu informieren?

Das Bundeskartellamt hat zunächst die Ausgangssituation bei Datensicherheit und Datenschutz und das wettbewerbliche Umfeld der Branche untersucht. Ein Schwerpunkt lag auf den technischen Grundlagen und Methoden des Messaging und des Audio-/Video-Austauschs. Die technischen Gegebenheiten und Praktiken bei den einzelnen Diensten beeinflussen nicht nur die **Datensicherheit und die (rechtskonforme) Umsetzung Datenschutzmaßnahmen**. Die technische Infrastruktur kann sich auch auf Wettbewerbsprozesse auswirken. Sie ist somit auch maßgeblich für das Ziel des Bundeskartellamts, Datenschutz als Wettbewerbsparameter zu fördern.

Von ihr hängt beispielsweise ab, ob und inwieweit der Zugang und der Anschluss an andere Messenger- und Video-Systeme oder die Integration technischer Innovationen in ein System möglich ist. Die Komplexität der technischen Infrastruktur und Verfahren dürften auch die Initiative der Verbraucherinnen und Verbraucher beeinträchtigen. Ihre Bereitschaft, Datenschutz wie oben beschrieben als Auswahlkriterium zu nutzen, setzt zunächst ein grundlegendes Verständnis der anspruchsvollen technischen Zusammenhänge voraus. Die **Perspektive der Verbraucherinnen und Verbraucher** ist entscheidend für jegliche Handlungsempfehlungen. Es sind Rahmenbedingungen zu

schaffen und Anreize zu setzen, um sie und die anbietenden Dienste zu motivieren, dem Datenschutz im Wettbewerb eine höhere Priorität einzuräumen.

Das Bundeskartellamt hat über 40 verschiedene Dienste zu diesen Themen befragt und eine Reihe von Expertengesprächen geführt. Darüber hinaus wurde eine Vielzahl von Studien und Fachartikeln ausgewertet.

#### *Verlauf und weitere Themen*

Im **Zwischenbericht**, der im November 2021 veröffentlicht wurde, hat das Bundeskartellamt die Ermittlungsergebnisse aus zwei untersuchten Themenbereichen dargelegt: Zum einen wurde ein Überblick über die Rahmenbedingungen der **Branche** sowie die verschiedenen Anbietergruppen, Funktionalitäten und Geschäftsmodelle gegeben. Zum anderen wurden die ersten Ergebnisse der Unternehmensbefragung zur **Interoperabilität** dargestellt. Es wurde hinterfragt, inwieweit eine solche Interoperabilität die Datensicherheit und damit das Datenschutzniveau von Messenger- und Video-Diensten beeinflussen würde und in welchem Ausmaß mit Auswirkungen auf Innovationsanreize und die Wettbewerbsintensität in der Branche zu rechnen ist.

In diesem **Abschlussbericht** hat das Bundeskartellamt die vorgenannten Ausführungen um die Erkenntnisse zum Thema Datenschutz bei Messenger- und Video-Diensten, insb. um **Kriterien der Datensicherheit und der Datenverarbeitung** erweitert. Die Ermittlungsergebnisse werden dargelegt, eingeordnet und rechtlich überprüft. Des Weiteren werden die bis hierher noch ausstehenden Ermittlungsergebnisse zur **Interoperabilität**, die sich insb. auf die technische Umsetzung und Gestaltung richten, dargestellt und mit den entsprechenden Regelungen des **Digital Markets Act (DMA)**, der zwischenzeitlich am 1. November 2022 in Kraft getreten ist, in Beziehung gesetzt. Vor diesem Hintergrund werden **Ansätze für mehr wettbewerblichen Datenschutz** entwickelt, die sich sowohl auf die Verbraucherinnen und Verbraucher als auch auf die Dienste richten. Darauf aufbauend schließt der Bericht mit **Empfehlungen** zur Verbesserung des Datenschutzniveaus bei Messenger- und Video-Diensten in Deutschland. Hier werden nicht nur die rechtlichen Bedingungen, Ausschreibungs- und Förderungspraktiken und die Situation des öffentlichen Bereichs angesprochen. Es wird angeregt, die **Rahmenbedingungen für wettbewerblichen Datenschutz** zu verbessern und eine transparente Bewertung der Datenschutzqualität einzuführen.

#### *Kriterien der Datensicherheit und Datenverarbeitung bei Messenger- und Video-Diensten*

Das Bundeskartellamt hat sich für diese Sektoruntersuchung ausführlich mit den technischen Grundlagen des Messaging und des Audio-/Video-Austauschs beschäftigt. Es hat eine **Checkliste** mit den wesentlichen Kriterien für Datensicherheit und Datenschutz erstellt. Diese umfasst zunächst das **Protokoll** einschließlich der Ende-zu-Ende-Verschlüsselung auf dem Stand der Technik. Das Protokoll kann als Sprache eines Messaging- und Video-Systems verstanden werden, dass die Regeln für den

Austausch und den Anschluss an das System umfasst. Die **Ende-zu-Ende-Verschlüsselung** sorgt dafür, dass der Datenaustausch vom Sender bis zum Empfänger von niemand anderem gelesen werden kann als von den Kommunizierenden selbst. Verschlüsselung macht nur Sinn, wenn auch die Identität der Nutzerinnen und Nutzer, die die verschlüsselten Daten austauschen, eindeutig ist. Mit der **Zwei-Faktor-Authentisierung** können die Verbraucherinnen und Verbraucher die eigene Identität gegenüber ihrem Messenger- und Video-Dienst sowie gegenüber ihren Kommunikationspartnerinnen und -partnern absichern.

Verwenden Dienste generell **internationale technische Standards** geht damit ein gewisses überprüfbares Qualitätsniveau einher. Zudem kann Interoperabilität einfacher hergestellt werden, wenn sich die Kommunikation auf identischen technischen Prinzipien gründet. Wenn der **Quellcode eines Messenger- und Video-Dienstes einsehbar** ist, können kompetente Dritte die Datensicherheit des Systems überprüfen. Ist dies nicht der Fall, sollte es die Möglichkeit geben, dass zumindest Sicherheitsaudits durch unabhängige renommierte Prüfinstitutionen durchgeführt und veröffentlicht werden. Sofern die Datenschutzerklärung nicht gelesen wird, kann die Art des Geschäftsmodells ein Indiz dafür sein, ob Daten eine ungewisse Weiterverwendung finden oder nicht. Hier ist auf **Datensparsamkeit** zu achten. Wenn Nutzerinnen und Nutzer **Konten** anlegen müssen, wie es bei Diensten großer Konzerne, die ein digitales Ökosystem betreiben, der Fall ist, werden viele Daten bereits dadurch erfasst.

Messenger- und Video-Dienste sollten die Daten von EU-Bürgerinnen und -Bürgern **im Geltungsbereich der DSGVO speichern** und nicht in andere Jurisdiktionen transferieren, um die Datensicherheit rechtskonform zu bewahren. Dies betrifft insbesondere den Vergleich mit den USA, wo die Geheimdienste auf dort gespeicherte Daten der Verbraucherinnen und Verbraucher zugreifen können. Verbraucherinnen und Verbraucher können ihre Daten und diejenigen ihrer Kontaktpersonen schützen, wenn sie auf die Synchronisation des **Kontaktverzeichnisses verzichten**, bzw. ihren Dienst dementsprechend auswählen oder anweisen.

Die Ermittlungsergebnisse waren nach mehreren Maßstäben zu bewerten. Zunächst war zu überprüfen, ob die Kriterien der Datensicherheit und des Datenschutzes entsprechend dem **Stand der Technik** umgesetzt werden und zukunftsfähig sind. Diese Frage gewann vor dem Hintergrund einer möglichen Interoperabilität von Messenger- und Video-Diensten und ihrer Auswirkungen auf Datenschutz und Datensicherheit an Bedeutung. Kurz vor Abschluss der Sektoruntersuchung – im November 2022 – ist der DMA mit einem **Interoperabilitätsregime** für Gatekeeper in Kraft getreten, womit sich das rechtliche Umfeld in dieser Frage konkretisiert hat. Schließlich war die **Wahrnehmung der Verbraucherinnen und Verbraucher** einzubeziehen. Verschiedene Verbraucherbefragungen und wissenschaftliche Untersuchungen lassen keine eindeutigen Rückschlüsse zu, inwieweit die Verbrauchenden in der Lage und willens sind, sich komplexe technische Hintergründe zu erarbeiten

und in datenschutzfreundliche Auswahlstrategien umzusetzen. Auch ob und inwieweit die **Information und Präsentation datenschutzrelevanter Fakten** durch die Dienste geeignet ist, die Verbrauchenden „einzufangen“, ist fraglich. Zweifel scheinen hier angesichts der gegenwärtigen Marktverfassung und der fortbestehenden starken Position bekannter Dienste angebracht.

Nach dem Ergebnis der Ermittlungen existiert in der Branche der Messenger- und Video-Dienste viel **Innovationskraft und Expertise** in Sachen Unabhängigkeit und Schutz der persönlichen Daten der Nutzerinnen und Nutzer. Allerdings sind in der Branche gleichzeitig **verschiedene Praktiken zu bemängeln**. Die Ergebnisse der Sektoruntersuchung legen den Schluss nahe, dass verschiedene Dienste Engagement vermissen lassen und die Expertise und Möglichkeiten nicht so umsetzen, wie es aus Sicht der Nutzerinnen und Nutzer wünschenswert und möglich wäre. Dies lässt sich aber nur schwer an einzelnen Gruppen von Diensten festmachen. So schneiden nach den Ermittlungsergebnissen zwar freie Messaging-Systeme und Open Source-Dienste bei einer Vielzahl der Kriterien gut ab. Allerdings ist die Frage, wie Datensicherheit im Detail gestaltet wird, hier letztendlich vom ausgewählten (Server-) Betreiber abhängig. Generell eröffnen sich den Nutzerinnen und Nutzern bei den meisten Diensten **viele Wahlmöglichkeiten**, die teilweise ein gewisses Bewusstsein für sicherheitsrelevantes Handeln erfordern, wie z. B. - wie eben erwähnt - die **Auswahl des Serverbetreibers** oder generell auch die **Aktivierung der Ende-zu-Ende-Verschlüsselung**.

Umgekehrt können Verbraucherinnen und Verbraucher, wenn sie bereit sind, sich zu informieren, ein **weites Feld an Möglichkeiten** vorfinden, um ihren Messenger so zu gestalten bzw. den Client zu finden, der ihre Anforderungen am besten erfüllt und aufgrund von Datensparsamkeit und der Verwendung internationaler Standards auch im Hinblick auf Interoperabilität zukunftsfähig ist. Auch einige Videokonferenzdienste bieten ihren Nutzerinnen und Nutzern viele Optionen. In weiten Teilen ist das der Ausrichtung auf die Wünsche von Geschäftskundinnen und Geschäftskunden geschuldet. Ein hohes Sicherheitsniveau kann umgesetzt werden. Letztendlich liegt sicherheitsbewusstes Handeln aber häufig in der **Verantwortung des jeweiligen Host** oder der Administratorin oder des Administrators, unabhängig davon, ob diese Rolle geschäftlich oder privat ausgeführt wird.

Was die zu bemängelnden Praktiken oder das fehlende Engagement angeht, so betrifft dies zum einen die **Verschlüsselung**. Einzelne bekannte Messenger- und Video-Dienste überraschen damit, dass sie Sicherheit **nicht auf dem Stand der Technik** umsetzen und es zum Beispiel bei einer Transportverschlüsselung belassen oder die Ende-zu-Ende-Verschlüsselung nur bei bestimmten Funktionen einsetzen, was nicht mit technischen Restriktionen begründet werden kann. Ferner wäre es wünschenswert, dass branchenweit weitere Sicherheitsverfahren, wie die Verschlüsselung der Daten auf dem Endgerät, die Ablageverschlüsselung, die Zwei-Faktor-Authentisierung sowie Backups in der Branche einen höheren Verbreitungsgrad hätten. Des Weiteren sei auf die rechtliche Analyse

verwiesen. Einige Dienste **speichern Daten europäischer Nutzerinnen und Nutzer außerhalb des Geltungsbereichs der DSGVO**, was rechtlich nicht zulässig ist, oder der genaue Speicherort bleibt unklar. Auch die **Synchronisation des Kontaktverzeichnisses** in Folge derer Daten Dritter verarbeitet werden, wird von verschiedenen Diensten betrieben und kann unzulässig sein.

### *Rechtliche Einordnung*

Das Bundeskartellamt hat von den Messenger- und Video-Diensten zunächst sowohl zur Datenspeicherung und zum Datentransfer als auch zur Synchronisation des Kontaktverzeichnisses Auskünfte verlangt und die Ergebnisse einer rechtlichen Analyse unterzogen. Nach den Ermittlungsergebnissen liegen **Verstöße einiger Messenger- und Video-Dienste** gegen die Vorschriften der DSGVO nahe.

Die **Synchronisation des Kontaktverzeichnisses** führt dazu, dass auch die Kontaktdaten von Nicht-Nutzerinnen und Nicht-Nutzern erfasst werden. Nach derzeitiger Auffassung des Bundeskartellamts entspricht diese gängige Praxis vieler bekannter Messenger- und Video-Dienste nicht den Anforderungen von Art. 6 Abs. 1 Unterabs. 1 Buchst. a) DSGVO, sofern sie dauerhaft erfolgt. Der Personenbezug der Daten besteht fort, auch wenn die Telefonnummer durch einen kryptographischen Hashwert ersetzt wird, der mit der Nutzerin oder dem Nutzer verknüpft ist, aus deren Kontaktverzeichnis die Telefonnummer stammt. Aus der Wahrung berechtigter Interessen ergibt sich keine weitere Legitimation des Verantwortlichen, da der Vernetzungsvorteil zu gering erscheint.

Die Ermittlungsergebnisse zum Prozess der Datenverarbeitung legen nahe, dass sich einige Messenger- und Video-Dienste beim **Datentransfer in Drittländer und beim Speichern auf Servern in Drittländern** (Art. 45 DSGVO) nicht rechtskonform verhalten. Dies betrifft vor allem diejenigen Dienste, die Daten deutscher Nutzerinnen und Nutzer in den USA speichern. In Länder außerhalb der EU und des Europäischen Wirtschaftsraums dürfen Daten nur übermittelt werden, wenn ein angemessenes Datenschutzniveau in dem jeweiligen Drittland (Art. 45 DSGVO) sichergestellt ist. Allerdings ist der frühere Datenschutzschild (EU-US Privacy Shield), den die EU mit den USA verhandelt hatte, nach dem „*Schrems II*“ - Urteil des EuGH aus dem Sommer 2020 ungültig. Neben möglichen Verstößen gegen die DSGVO war ein weiteres rechtliches Untersuchungsfeld eine mögliche Irreführung der Verbraucherinnen und Verbraucher durch **Informationsmängel** (§ 5a Abs. 1 UWG) **bei der Ende-zu-Ende-Verschlüsselung**. Hier dürfte sich nach Auffassung des Bundeskartellamts ein Transparenzverstoß durch Informationsmängel in Bezug auf die Verschlüsselungsart nicht leicht begründen lassen. Für einen möglichen Verstoß gegen das Transparenzgebot des UWG müsste die „geschäftliche Relevanz“ von Sicherheitseigenschaften wie der Ende-zu-Ende-Verschlüsselung begründet werden. Allerdings ist die Marktentwicklung seit der Konzipierung der Sektoruntersuchung vorangeschritten. Die Ende-zu-Ende-Verschlüsselung hat sich

als Branchenstandard etabliert, so dass es hinsichtlich dieser Sicherheitseigenschaft keinen Unterschied machen dürfte, wo Nutzerinnen und Nutzer sich registrieren. Vor diesem Hintergrund war überraschend, dass einige wenige bekannte Dienste die Ende-zu-Ende-Verschlüsselung nicht oder nur eingeschränkt umsetzen. Eine bessere Einschätzung der Sichtweise der Verbraucherinnen und Verbraucher hätte weiteren Ermittlungsaufwand wie etwa eine Verbraucherbefragung erfordert, mit welchem aufgrund der Komplexität der Begrifflichkeiten aber nur ungewisse Aufklärungschancen verbunden gewesen wären. Auch die Einordnung des Verhaltens der Verbrauchenden aus Unternehmenssicht blieb uneindeutig, da es viele kostenfreie Angebote der Messenger- und Video-Dienste gibt. Letztendlich musste eine abschließende Bewertung jeweils der **Klärung im Einzelfall** vorbehalten bleiben.

### *Interoperabilität*

Mit Inkrafttreten des Digital Markets Act im November 2022 hat sich das rechtliche Umfeld der Messenger- und Video-Dienste in Sachen Interoperabilität geklärt. Wegen der anhaltenden rechtspolitischen Diskussion über eine gesetzliche Verpflichtung von Messenger- und Video-Diensten zur Interoperabilität hatte das Bundeskartellamt in seiner Untersuchung den befragten Unternehmen **bereits vor der Einigung im Trilog zum DMA im März 2022** auch zu diesem Themenkomplex Fragen gestellt. Wie im Zwischenbericht bereits ausführlich dargelegt, hatte die Befragung der Unternehmen durch das Bundeskartellamt dabei einen klaren Fokus. Es ging darum, den verschiedentlich geäußerten Erwartungen nachzugehen, dass durch Interoperabilität der Wechsel zu datenschutzfreundlichen Messenger-Diensten erleichtert und dadurch die **Datenschutzqualität** in diesem Bereich gefördert wird. Andere mit Interoperabilität verbundene Zielvorstellungen, wie etwa die Sicherstellung von Konnektivität im Bereich der interpersonellen Kommunikation oder ein Abbau von Marktmacht führender Messenger-Dienste, waren kein direkter Gegenstand der Untersuchung. Als wesentliche **Einflussgrößen** für Datenschutzeffekte durch Interoperabilität konnten nach den im Zwischenbericht dargelegten Ermittlungsergebnissen die technischen Erfordernisse, die Ausgestaltung der Datensicherheit, die Wechselwirkungen von Interoperabilität im Hinblick auf Innovationsanreize und die Wettbewerbsintensität sowie das Verbraucherverhalten gesehen werden. Insgesamt hatte die Befragung gezeigt, dass Interoperabilität von den betroffenen Unternehmen nicht rundheraus abgelehnt wird. Vielmehr werden in Teilbereichen Interoperabilität oder zumindest Formen des Austausches in unterschiedlicher technischer Tiefe und Reichweite bereits praktiziert. In Standardisierungsgremien werden technische Grundlagen für Interoperabilität in globalem Kontext erarbeitet. Dies ging allerdings einher mit der klaren Haltung eines Großteils der Branche, dass eine gesetzliche Verpflichtung zur branchenweiten Interoperabilität mehr schaden als nützen würde und insofern abzulehnen sei. Für den Fall einer erzwungenen Interoperabilität befürchteten die Unternehmen mit einer ablehnenden Haltung insbesondere negative Effekte auf die

Innovationstätigkeit und damit auch auf das Datensicherheits- und Datenschutzniveau beim Messaging und Videoconferencing.

Das Bundeskartellamt hatte herausgestellt, dass die Erkenntnisse aus der Branchenbefragung belegen, wie vielschichtig und komplex die **Analyse der Wirkungszusammenhänge rund um das Thema Interoperabilität** ist. Bei der Umsetzung sollten nicht nur die notwendigen Investitionen in technische Veränderungen der Dienste oder die Entwicklung technischer Neuerungen berücksichtigt werden. Ebenso einzubeziehen wären mögliche positive oder negative Wohlfahrtseffekte durch veränderte Innovationsanreize und Auswirkungen auf Geschäftsstrategien und Wettbewerbsintensität.

Nach **dem in Art. 7 DMA normierten Konzept einer Interoperabilitätsverpflichtung** sind lediglich designierte Gatekeeper unter den Messenger-Diensten Adressat der Verpflichtung. Des Weiteren lebt die Verpflichtung erst auf, sobald sich ein anderer Dienst mit einem entsprechenden Petitum (freiwillig) an den Gatekeeper wendet. Schließlich sind lediglich die Basisfunktionen von der Verpflichtung umfasst. Nichtsdestotrotz dürften die damit einhergehenden praktischen Herausforderungen erheblich sein. Die Datensicherheit muss technisch auch unter Interoperabilität gewährleistet werden. Aufgrund der vielfältigen individuellen Lösungen der Dienste und technischer Herausforderungen bleibt eine **marktweit interoperable Ende-zu-Ende-Verschlüsselung** bisher eine Herausforderung. Zusätzlich sind zahlreiche datenbezogene Schwierigkeiten zu überwinden. Dies betrifft z. B. die **Datenüberwachung und -verantwortung**, wenn diese durch mehr Hände gereicht werden. Bei unterschiedlichem Umgang mit Kontaktverzeichnis und Datenspeicherung unter den Diensten muss **jederzeit rechtskonformes Verhalten** sichergestellt werden. Ob und inwieweit **Innovationschancen** erhalten werden können, ist eine komplexe Frage, die nicht theoretisch gelöst werden kann. Nach den Erkenntnissen aus den Ermittlungen sind hier durchaus Zweifel angebracht. Zwar ist das DMA-Interoperabilitätsregime auf Basisfunktionen beschränkt. Allerdings sind die Architektur der Dienste und die technische Verortung der einzelnen Funktionen auf dieser sehr individuell, so dass Interoperabilität hier Vereinheitlichungen und Anpassungen in unterschiedlichem Ausmaß erfordern würde, was auch die Innovationskräfte unterschiedlich beeinträchtigen könnte. Die Bewertung ist letztendlich abhängig vom unterstellten Entwicklungsszenario. Wenn es nur zu einzelnen oder wenigen **bilateralen Vereinbarungen** zwischen Gatekeepern und Petenten käme, erscheinen die Herausforderungen lösbar, zumal die Erschwernisse auf Seiten der Petenten freiwillig in Kauf genommen werden. Eine Vielzahl von individuellen Referenzangeboten erscheint dagegen aus gesamtwirtschaftlicher Perspektive nachteilig, so dass dann über entsprechende marktweite Standardisierungen beraten werden müsste. Letzteres erscheint nach den Ermittlungsergebnissen des Bundeskartellamts zum jetzigen Zeitpunkt wenig wahrscheinlich. Nicht auszuschließen ist, dass



die Interoperabilitätsverpflichtung für Gatekeeper **Neueinsteigern Chancen bietet**, die auf den Anschluss an die großen Netzwerke führender Dienste angewiesen sind.

#### *Ansätze für mehr wettbewerblichen Datenschutz*

Die Datenschutzqualität scheint insb. auf Seiten der Verbraucherinnen und Verbraucher als Nachfragende und auch bei einigen Diensten nicht die notwendige Beachtung innerhalb wettbewerblicher Auswahlprozesse zu finden. Es dürfte somit nicht davon auszugehen sein, dass sich das Datenschutzniveau unter den gegebenen Rahmenbedingungen marktgetrieben verbessern wird. Vielmehr sind zum einen datenschutzfreundliche Dienste im Wettbewerb zu stärken. Zu hinterfragen ist zum anderen, welche Anreize notwendig sind, damit die Verbraucherinnen und Verbraucher die Datenschutzqualität als wesentliche Produkteigenschaft erkennen und zu datenschutzfreundlichen Diensten wechseln.

Wettbewerber etablierter Dienste haben auf **diskriminierende Ausschreibungsbedingungen** für Messaging und Video-Dienstleistungen mit sachlich unnötigen Hürden verwiesen. Hier wäre zu überprüfen, welche Bedingungen für die gewünschte Funktionserfüllung tatsächlich erforderlich sind. Eine weniger restriktive Handhabung darüberhinausgehender Anforderungen, z. B. an Größe und Umsatz, könnte ggf. datenschutzfreundlichen Diensten den Weg ebnen.

Viele der befragten Dienste versprechen sich auch von einer Überprüfung der aktuellen **Förderungspraxis von Open Source und Standardisierung** positive Effekte auf das Datenschutzniveau. Zugunsten der Sicherheit der Daten der Nutzerinnen und Nutzer könnte der gesamte Lebenszyklus einer Software einbezogen werden. Nicht nur die neu entwickelte Anwendung oder Technik als Innovation, sondern auch die kontinuierliche Wartung und Pflege der auf dieser Basis am Markt etablierten und von den Verbraucherinnen und Verbrauchern genutzten Produkte erscheint im Sinne der Datensicherheit förderungswürdig.

Wenn der öffentliche Bereich darüber hinaus ausschließlich datenschutzfreundliche Dienste einsetzen würde, wäre dies nach Ansicht vieler Befragter ein positives Signal für den Datenschutz. Allerdings legen die Erkenntnisse des Bundeskartellamts nahe, dass hier noch Verbesserungsmöglichkeiten bestehen könnten. Datenschutzfreundliche Messenger- und Video-Dienste haben sich bisher offenbar – sowohl, was ihre Auswahl als auch ihren bezahlten Einsatz im öffentlichen Bereich betrifft – nicht gegenüber weit verbreiteten Diensten durchsetzen können. Branchenvertretende haben zahlreiche Beispiele vorgelegt, wieviel Einsatz und Überzeugungskraft notwendig ist, damit datenschutzfreundliche Messenger- und Video-Dienste, die weniger bekannt sind als die etablierten Dienste, in Erwägung gezogen werden. Dies betrifft vor allem Bereiche, wo viele Verbraucherinnen und Verbraucher erreicht werden sollen, wie z. B. im öffentlichen Rundfunk,

aber auch bei Städten und Gemeinden, Bundesministerien oder Verwaltungseinheiten sowie im Bildungsbereich.

Was **Datenschutz als Qualitätseigenschaft** angeht, ist bisher nicht ersichtlich, dass viele Verbraucherinnen und Verbraucher die Auswahl ihres Messenger- und Video-Dienstes nach dessen Datenschutzfreundlichkeit richten. Wenn sie es doch versuchen, müssen sie mit sehr ungleich verteilten Informationen - zugunsten der Dienste, zu ihren Lasten - zurechtkommen. Die Verbraucherinnen und Verbraucher müssten zunächst herausfinden, welche Informationen überhaupt relevant sind, dann diese suchen, sich ein grundlegendes Verständnis erarbeiten und abschließend aus mehreren Kriterien noch ein Gesamturteil bilden und vergleichen. In einer **technisch basierten Branche** scheinen sich unüberwindbare Hürden zu stellen: Die technischen Kriterien, Verfahren und Praktiken, die die Datenschutzqualität eines Messenger- und Video-Dienstes bestimmen, sind für Laien komplex und schwer nachzuvollziehen. Die Messenger- und Video-Dienste verspüren dadurch - jedenfalls abseits des Geschäftskundensegments - wenig Druck, den Verbraucherinnen und Verbrauchern eine informierte Entscheidung in Sachen Datenschutz zu ermöglichen.

Im Zuge aktueller Entwicklungen treten weitere Herausforderungen hinzu: Die Interoperabilitätsregeln im DMA werden die Datensicherheit und damit den Datenschutz vor weitere Herausforderungen stellen. Die Dienste sind technisch unterschiedlich aufgestellt. Viele bekannte Dienste sind als geschlossenes System gestaltet worden. Die Daten der Nutzerinnen und Nutzer können somit neuen Risiken ausgesetzt sein. Dieser Umstand erfordert hohe Aufmerksamkeit, wenn Interoperabilität praktiziert wird. Allerdings kann die Informationslage für die Verbraucherinnen und Verbraucher gleichzeitig noch undurchschaubarer werden.

*Die **Komplexität der notwendigen Informationen kann am Beispiel der Verschlüsselung** veranschaulicht werden, auch wenn vereinfachend von tieferen technischen Details und Benennungen abgesehen wird. So sind zunächst verschiedene **Varianten** der Verschlüsselung zu unterscheiden. Bei der Transportverschlüsselung wird der Transportkanal einer Nachricht verschlüsselt. Sie kann aber sowohl von Nutzerinnen und Nutzern des Messenger- und Video-Dienstes selbst, als auch vom Serverbetreiber eingesehen werden. Anders als bei der Transportverschlüsselung wird bei der Ende-zu-Ende-Verschlüsselung („E2E-Verschlüsselung“) die Nachricht verschlüsselt über alle Übertragungsstationen hinweg versendet. Nur die Kommunikationspartner als Endpunkte der Kommunikation können die Daten entschlüsseln. Beide Varianten können jeweils einzeln oder kombiniert eingesetzt werden. Letzteres bietet das höchste Sicherheitsniveau. Zur Verschlüsselung kommen **verschiedene kryptographische Verfahren** wie die symmetrische oder die asymmetrische Verschlüsselung mit öffentlichen und privaten Schlüsseln zum Einsatz. Die Ende-zu-Ende-Verschlüsselung wird in der Praxis über unterschiedliche technische Standards umgesetzt, je nachdem, welche Kommunikationsform - Textnachricht, Audio-/Video-Austausch - verwendet wird und welches Messaging- und Video-System genutzt wird. Darüber hinaus bestehen bisher **zahlreiche technische Einschränkungen**, die auch einer möglichen Interoperabilität im*

Wege stehen würden. Dies betrifft zum einen die Verschlüsselung von **Textnachrichten in Gruppen (Gruppenchat)**, die mit ansteigender Gruppengröße immer aufwendiger wird. Die Lösung in Form des neuen Standards Messaging Layer Security (MLS) wird vereinzelt erprobt. Außerdem wurde eine neue Arbeitsgruppe bei der IETF eingesetzt, die Lösungen für interoperables Messaging entwickeln soll und dazu auch den MLS-Standard verwenden wird. Ob und inwieweit sowie wann es zu einer flächendeckenden Umsetzung in der Branche kommt, ist abzuwarten.

Auch bei **Videokonferenzen und Webinaren** unterliegt die Ende-zu-Ende-Verschlüsselung zurzeit technischen Einschränkungen. Generell erfordert die Ende-zu-Ende-Verschlüsselung, dass die Teilnehmenden technisch in der Lage sind, die notwendigen Verschlüsselungsfunktionen bereitzustellen und anzuwenden. Alle Teilnehmenden müssen sich auf dem gleichen Sicherheitsniveau bewegen. Im Umkehrschluss kann eine E2E-Verschlüsselung nicht erreicht werden, sobald eine Teilnehmerin oder ein Teilnehmer das geforderte Sicherheitsniveau unterschreiten. Dieser Fall tritt z. B. dann ein, wenn Teilnehmende einen sogenannten **WebRTC-Client** einsetzen. WebRTC ist ein direkt im Browser verankertes Protokoll, welches nur zwischen zwei Endpunkten Ende-zu-Ende verschlüsseln kann. Bei mehr als zwei Teilnehmenden einer Videokonferenz sind dies jeweils das Endgerät der Nutzerin oder des Nutzers mit dem Server des Dienstes, was den Anforderungen der Ende-zu-Ende-Verschlüsselung nicht mehr entspricht.

Auch mit bestimmten **Funktionen**, die Nutzerinnen und Nutzer in Videokonferenzen gerne verwenden, kann die Ende-zu-Ende-Verschlüsselung derzeit technisch nicht verbunden werden: Zu diesen Funktionen gehören z. B. die **Einwahl aus dem öffentlichen Telefonnetz** oder die **Aufzeichnung von Meetings** durch den anbietenden Dienst. Dies ist nur möglich, wenn der Dienstbetreiber auf den Datenstrom zugreifen kann, um den Audioanruf einzubinden bzw. die Daten aufzuzeichnen. Auch die **Anbindung bestimmter externer Geräte** (z. B. Raumkonferenzsystem-Geräte, die auf dem SIP-Protokoll basieren) ist unter Ende-zu-Ende-Verschlüsselung nicht möglich, da dazu die verschiedenen Protokolle synchronisiert werden müssten. Führende Dienste haben auf eben solche und weitere Einschränkungen, wie beispielsweise die **Verwendung von „Assistenten“** ausdrücklich hingewiesen.

Große Videokonferenzen für **Webinare mit mehreren Hundert Teilnehmenden** können zurzeit technisch nicht durch Ende-zu-Ende-Verschlüsselung gesichert werden. In diesem Anwendungsfall ist es notwendig zu prüfen, ob der anbietende Dienst einen Video-Dienst-Standort in Deutschland betreibt und dieser sicherheitstechnisch geprüft wurde (beispielsweise durch ein BSI C5 Testat). Transportverschlüsselung und der sichere Betrieb des Video-Dienstes in Deutschland sollten hierfür das Kriterium sein. Ferner ist darauf zu achten, dass die Identität der Teilnehmenden zweifelsfrei festgestellt werden kann („Authentisierung“). Ende-zu-Ende-Verschlüsselung stellt die Integrität der übermittelten Daten sicher. Ohne eine vorherige zweifelsfreie Authentisierung sorgt sie zwar für den Schutz der übermittelten Daten, stellt aber nicht sicher, wer diese Daten empfangen kann.

In der Checkliste des Bundeskartellamts, die einer Einschätzung der Datenschutzqualität von Messenger- und Video-Diensten zugrunde gelegt werden könnte, ist die **Verschlüsselung nur eines von mehreren Kriterien**, die sich die Verbraucherinnen und Verbraucher erschließen müssten. Vor diesem Hintergrund erscheint es nicht zumutbar und zielführend, die Verantwortung für mehr wettbewerblichen Datenschutz allein den Verbraucherinnen und Verbrauchern zuzuordnen, auch

dann nicht, wenn die Informationen für die Verbrauchenden extrem komprimiert und vereinfacht würden. Maßnahmen zugunsten der Datenschutzqualität müssen auch die Dienste einbeziehen. An die Seite einer effektiven Durchsetzung des geltenden Rechts sollten daher Maßnahmen gestellt werden, die den Datenschutz als Wettbewerbsparameter stärken können.

#### *Datenschutzqualität vergleichend und transparent bewerten*

Nach derzeitiger Auffassung des Bundeskartellamts könnten rein marktbezogene Maßnahmen nicht ausreichend sein, um Datenschutz aus seinem Schattendasein unter den Wettbewerbsparametern herauszuhelfen und die notwendige Aufmerksamkeit zu verschaffen. Eine transparente und vergleichende Bewertung der Datenschutzqualität von Messenger -und Video-Diensten, z. B mit Hilfe eines Rating-Verfahrens anhand ausgewählter Kriterien des Datenschutzes und der Datensicherheit, könnte hilfreich sein.

**Ein solches Verfahren könnte beide Marktseiten** in Sachen Datenschutz aktivieren. Die größte Resonanz dürfte es zunächst auf der Seite der anbietenden Messenger- und Video-Dienste auslösen. Es darf vermutet werden, dass viele Messenger- und Video-Dienste ein **öffentlich negatives Zeugnis oder ein schlechteres Ranking als der wichtigste Wettbewerber** vermeiden möchten. Datenschutz ist nicht nur „Gesetz“ - in Deutschland und Europa in Gestalt der DSGVO - sondern inzwischen auch zu einem sensiblen Thema geworden, das von der (Fach-) Öffentlichkeit aufmerksam verfolgt wird und auch im politischen Umfeld Beachtung findet. Dazu hat auch die ständige Auseinandersetzung mit den Praktiken einiger führender Branchenvertreter und öffentliches Nachdenken über staatliche Initiative wegen unerwünschter Praktiken und Entwicklungen beigetragen. Möglicherweise möchten aber auch die Verbraucherinnen und Verbraucher nicht bei einem Messenger- und Video-Dienst registriert sein, der **im Ranking den letzten Platz** einnimmt. Vielleicht möchte auch eine ihrer Kontaktpersonen lieber einen Messenger- und Video-Dienst nutzen, der ein niedrigeres Datenschutzrisiko aufweist als der bisher gewählte Dienst. Dies gilt auch, wenn stellvertretend für die Verbrauchenden agiert wird: Ein veröffentlichtes Rating-Urteil einer vertrauenswürdigen Instanz kann die **glaubwürdige Information sein, die berufliche „Entscheider“ oder Ansprechpartner** für die Öffentlichkeit bei Behörden und Unternehmen benötigen, um über die DSGVO-Konformität eines Messenger- und Video-Dienstes und damit dessen Einsatzmöglichkeiten in der eigenen Institution zu entscheiden.

#### *Das Bundeskartellamt empfiehlt in Anknüpfung an den vorliegenden Bericht:*

- Die **Durchsetzung des Verbraucherrechts sollte gestärkt** werden. Die digitale Wirtschaft stellt die Verbraucherinnen und Verbraucher insb. aufgrund ihrer technischen Basis ständig vor neue Herausforderungen, die trotz des Engagements aller Akteure immer schwerer einzufangen sind. Die Kompetenzen und Erfahrungen des Bundeskartellamts bei der

Rechtsdurchsetzung können hier einen sinnvollen Beitrag zur Bewältigung und Gestaltung leisten.

- Die Bemühungen um die Aufklärung der Verbraucherinnen und Verbraucher, insb. zugunsten der Entwicklung von Medienkompetenz, sind zu intensivieren. Alle Bevölkerungsgruppen sollten in eine **Kommunikationsstrategie für den Datenschutz** integriert werden. Eine entsprechende bundesweite Kampagne sollte daher sowohl die internetbasierten digitalen Medien als auch herkömmliche Medien, wie Fernsehen, nutzen.
- Ein denkbares Signal wäre, wenn der **öffentliche Bereich** datenschutzfreundliche Messenger- und Video-Dienste stärker einsetzen würde. Ansprechpersonen und Entscheiderinnen und Entscheider brauchen verlässliche Informationen **zur DSGVO-Konformität von Messenger- und Video-Diensten** – gerade auch derjenigen Dienste, die nicht im Fokus des öffentlichen Interesses stehen. Daher könnten Institutionen, Organisationen und Unternehmen den Mitarbeitenden entsprechende **schriftliche Informationsbriefe, -broschüren und Handreichungen** zur Verfügung stellen.
- **Interoperabilität** sollte nicht nur **innovationsfreundlich**, sondern auch **verbraucherorientiert** umgesetzt werden. Die ohnehin komplexen technischen und rechtlichen Zusammenhänge von Datensicherheit und Datenschutz dürften unter Interoperabilität noch weniger zu überblicken sein. Bei jeglichen Vorhaben und Bemühungen zur Gestaltung von Interoperabilität einschließlich ihrer technischen Herausforderungen dürfen die Verantwortlichen stellvertretend für die Nutzerinnen und Nutzer die **Anforderungen eines sicheren Verbraucherprodukts** nicht aus dem Blick verlieren.