

Marina Steenbergen

Metaverse – eine Datenschutzfalle?

Datenschutzrisiken und ihre Auswirkungen auf die Nutzungsbereitschaft für Metaverse-Anwendungen

Metaverse-Anwendungen könnten in Zukunft Teil unseres Alltags sein. Zugleich weisen Literatur und Organisationen bereits darauf hin, dass mit der Nutzung immersiver virtueller Welten auch Datenschutzrisiken verbunden sind. Motiviert durch die Ergebnisse einer empirischen Datenerhebung zum allgemeinen Interesse an der Nutzung solcher Anwendungen sowie nutzungshemmenden Ursachen analysiert der vorliegende Beitrag drei Risiken der Metaverse-Nutzung anhand von Risikofaktoren nach der DSGVO.

1 Metaverse-Anwendungen

In den letzten Jahren haben Metaverse-Anwendungen als digitale Umgebungen, in denen Nutzer miteinander interagieren, Freizeitaktivitäten ausüben oder arbeiten können, an Bedeutung gewonnen.¹ Unter der Betrachtung verschiedener Definitionsansätze und Begriffsbestimmungen, die sich über die Jahre von der ersten Vision eines alleinigen Metaverse bis hin zu verschiedenen, ersten Ausgestaltungen entwickelt haben, können Metaverse-Anwendungen als virtuelle Welten zusammengefasst werden, die Elemente unserer analogen Welt aufweisen und ergänzen. In diesen virtuellen Welten können Nutzer als persönliche Avatare miteinander kommunizieren, interagieren und nutzergenerierte Inhalte erleben.² Konkrete Einsatzzwecke von Metaverse-Anwendungen sind unterhaltende Aktivitäten wie Gaming und der Besuch virtueller Konzerte oder Shopping. Aber auch Prozesse in den Bereichen Industrie und Wirtschaft könnten in Metaverse-Anwendungen ausgelagert werden.

Das sogenannte *Metaverse Maturity Model*³ bestimmt anhand von Reifegraden, welche bereits bestehenden und aktuellen digitalen Plattformen ausreichend Merkmale eines Metaverse aufweisen, um als solche identifiziert werden können. Zu diesen Merkmalen zählen Persistenz⁴, Synchronität⁵, Skalierbarkeit⁶, Interoperabilität⁷, Wirtschaft, Verknüpfung der virtuellen und analogen Welt⁸, Immersion⁹ und das Bestehen nutzergenerierter Inhalte. Einen erhöhten Reifegrad weisen u. a. die folgenden drei Anwendungen auf, die danach bis jetzt als Metaverse betitelt werden können:¹⁰

- *Decentraland*, das sich besonders durch hohe Kommerzialisierung und ein Wirtschaftssystem durch virtuelle Verkaufsflächen auszeichnet, begleitet von der Möglichkeit, Gegenstände mit Kryptowährung zu erwerben, sowie der digitalen Präsenz einer Vielzahl analoger Unternehmen und Marken.¹¹
- *Roblox*, das aktuell hohe Nutzerzahlen aufweist und besonders von Kindern und Jugendlichen genutzt wird.¹² Durch die Mög-

1 Die diesem Beitrag zugrundeliegenden Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projektes PriMeta (Förderkennzeichen 16KIS2050K) sowie vom BMBF und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autorin wieder.

2 Weinberger, What Is Metaverse? – A Definition Based on Qualitative Meta-Synthesis, Future Internet 2022, 14 (11), 310.

3 Weinberger/Gross, A comparison of virtual worlds based on the metaverse maturity model, ITU J-FET 2023, Vol. 4/4, 537.

4 Persistenz beschreibt das langfristige, nachhaltige Bestehen von Effekten und Umwelteinflüssen in einem Metaverse, die durch dortige Handlungen entstehen und für andere Nutzer sichtbar werden, z. B. Zerstörungen oder Inbesitznahmen von virtuellen Gegenständen, s. hierzu Ball, Das Metaverse, S. 50 ff.

5 Ereignisse und Interaktionen im Metaverse finden für jeden Nutzer in Echtzeit statt.

6 Skalierbarkeit sieht vor, dass ein Metaverse von einer großen Anzahl Nutzern gleichzeitig genutzt werden kann.

7 Interoperabilität bezeichnet die Möglichkeit, dass der Avatar, Gegenstände und Erfolge in andere virtuelle Welten oder Metaversen übertragen werden können.

8 Die Verknüpfung umfasst Auswirkungen auf die virtuelle Welt durch Veränderungen in der analogen Welt – und umgekehrt.

9 Immersion oder ein immersives Erleben bezeichnet das „Eintauchen“ in die virtuelle Realität, sodass sich diese für Nutzer möglichst real anfühlt. Dieser Effekt kann durch VR-Zubehör wie Headsets verstärkt werden.

10 Weinberger/Gross, ITU J-FET 2023, Vol. 4/4, 537, 543 (Fn. 3).

11 Z. B. Deutsche Bank, s. Berger, Warum das Metaverse das Banking verändern könnte, https://www.db.com/what-next/digital-disruption/Metaverse/banking/index?language_id=3.

12 Roblox, Q3 2023 Supplemental Materials, https://s27.q4cdn.com/984876518/files/doc_financials/2023/q3/Q3-23-Supplemental-Materials-FINAL.pdf, S. 21 f.



Marina Steenbergen

ist wissenschaftliche Mitarbeiterin der Abteilung IPR am Fraunhofer-Institut für Sichere Informationstechnologie SIT und in ATHENE.

E-Mail:
marina.steenbergen@sit.fraunhofer.de

lichkeit, Gegenstände zu erwerben und zu handeln, weist es ausgeprägt kommerzielle Züge auf, die von Unternehmen der analogen Welt beeinflusst werden können.

- *Horizon Worlds*, das nur mit VR-Headset genutzt werden kann und bei dem der Fokus auf sozialen Interaktionen zwischen Nutzern liegt, z. B. durch eine Verwendung für Meetings im Arbeitsalltag.

2 Nutzungsinteresse und Bedenken potenzieller Nutzer

In einer grundsätzlich anonymen¹³ Online-Umfrage unter 100 Personen im Zeitraum vom 13.11.2024 bis 21.01.2025 wurden die Bekanntheit des Begriffs „Metaverse“ sowie das Nutzungsverhalten und die Nutzungsbereitschaft erhoben. Die Online-Umfrage wurde auf Basis eines zuvor erstellten und hinsichtlich Eindeutigkeit und Verständlichkeit validierten Fragenkatalogs durchgeführt. Die Fragenvalidierung erfolgte am 14.10., 15.10. sowie am 17.10.2024 unter Hinzuziehung dreier potenzieller Umfrageteilnehmenden per Videokonferenzsystem.

Unter den 100 Teilnehmenden identifizieren sich 44 Personen als männlich, 55 als weiblich und eine als divers. 64 Personen waren zum Zeitpunkt der Umfragedurchführung 19-30 Jahre alt, 17 Personen 31-44 Jahre, 17 weitere Personen 45-65 Jahre und 2 Personen 66 Jahre oder älter.

2.1 Bekanntheit und Nutzung

Zunächst wurden die Teilnehmenden gefragt, ob sie den Begriff Metaverse bereits kennen und wie vertraut sie mit diesem sind. Im Anschluss sollten die Teilnehmenden angeben, ob sie bereits ein Metaverse genutzt haben und in welchem zeitlichen Umfang sie sich vorstellen (könnten), ein solches zukünftig zu nutzen.

■ *Bekanntheit*

Von dem Begriff Metaverse bereits gehört zu haben bestätigten 82/100 Teilnehmende. 43/82 Teilnehmende meinten, den Begriff auch erklären zu können. 18/100 Teilnehmende gaben an, den Begriff nicht zu kennen.

■ *Nutzungsverhalten*

Nach Erklärung des Begriffs und Nennung der zuvor dargestellten Anwendungen als Beispiele sollten die Teilnehmenden beantworten, ob sie ein Metaverse bereits genutzt haben, was 20/100 Teilnehmende bejahten und 80/100 verneinten.

■ *Nutzungspotenzial*

Sodann wurden die Teilnehmenden gebeten, den *wöchentlichen* zeitlichen Umfang anzugeben, den sie sich für die Nutzung eines Metaverse zukünftig (weiterhin) vorstellen könnten. Während 40/100 der Teilnehmenden angaben, grundsätzlich kein Interesse an der Nutzung zu haben, könnten sich 29/60 Teilnehmende vorstellen, ein Metaverse für bis zu eine Stunde zu nutzen, 21/60 Teilnehmende würden ein solches 1-5 Stunden nutzen, 5/60 Teilnehmende für 5-10 Stunden und weitere 5/60 für mehr als 10 Stunden.

¹³ Die Teilnehmenden wurden am Ende der Umfrage nach ihrer Bereitschaft gefragt, an Folgebefragungen in Form von Interviews teilzunehmen, mit dem Hinweis, dass die Teilnahme freiwillig ist und die hierzu notwendige Angabe ihrer E-Mail-Adresse für die weitere Kontaktaufnahme zum Verlust der Anonymität ihrer bisherigen Antworten führt.

2.2 Nutzungshemmnisse

Weiterhin sollte die Umfrage ermitteln, inwiefern Datenschutzbedenken ein Nutzungshindernis darstellen. Jene 40/100 Teilnehmenden, welche die Nutzung eines Metaverse gänzlich ablehnen, wurden daher nach den Gründen hierfür befragt. Hierzu standen den Teilnehmenden fünf verschiedene, kumulativ wählbare Antwortmöglichkeiten zur Verfügung,¹⁴ ebenso wie die Möglichkeit, sonstige Gründe innerhalb eines Freitextfelds anzugeben.

Für 35/40 Teilnehmende ist ein mangelnder Bedarf und fehlender Mehrwert der Nutzung ausschlaggebender Grund, ein Metaverse nicht nutzen zu wollen. Datenschutzbedenken¹⁵ sind für 12/40 Teilnehmende ein Nutzungshindernis. Für 6/40 Teilnehmende stellt die Angst vor negativen sozialen Erfahrungen¹⁶ ein Hindernis dar. 3/40 Teilnehmende gaben an, sich zu alt oder zu jung für die Nutzung zu fühlen, und 1/40 Personen wolle sich nicht mit der Steuerung vertraut machen oder befürchte hierbei Komplikationen.

Darüber hinaus machten 12/40 Teilnehmenden von der Freitexteingabe Gebrauch. Die dort genannten sonstigen Gründe lassen sich weiteren Kategorien zuordnen: 4/40 Teilnehmende betonten, Erlebnisse lieber in der Realität machen zu wollen, wobei 4/40 weitere Teilnehmende die Zunahme von Virtualität und den Verlust von Realität für gefährlich halten oder befürchten. 3/40 weitere Teilnehmende sehen hohe Kosten als Grund an, ein Metaverse nicht nutzen zu wollen. 1/40 Teilnehmende/r hält das Metaverse zum aktuellen Zeitpunkt für noch nicht ausgereift genug.

3 Grenzen der Erhebung

Die Aussagekraft der Datenerhebung ist insbesondere hinsichtlich der relativ geringen Anzahl an Teilnehmenden, die Beschränkung auf den deutschen Sprachraum und das mehrheitlich junge Alter der Teilnehmenden beschränkt. Darüber hinaus ist bei der Bewertung der Datenschutzbedenken zu berücksichtigen, dass nur diejenigen Personen zu Hinderungsgründen der Metaverse-Nutzung befragt wurden, die ein Metaverse grundsätzlich nicht nutzen würden. Zukünftige Arbeiten können untersuchen, inwieweit Datenschutz und besonders Datenschutzbedenken im Zusammenhang mit Metaverse-Anwendungen von Nutzern tatsächlich wahrgenommen und wie Datenschutzrisiken in Metaverse-Anwendungen eingeschätzt werden.

4 Relevanz von Datenschutzbedenken im Metaverse

Die Ergebnisse der Online-Umfrage zeigen, dass Datenschutzbedenken für 60% der Nutzer zumindest kein absolutes Hindernis zur Nutzung darstellen, da solche grundsätzlich bereit sind, Zeit im Metaverse zu verbringen. Aber auch von den 40% der Teilneh-

¹⁴ Diese Antwortmöglichkeiten waren: „Ich habe keinen Bedarf bzw. sehe keinen Mehrwert“, „Ich fühle mich dafür zu alt oder zu jung“, „Ich möchte mich nicht mit der Steuerung vertraut machen oder denke, die Steuerung könnte mich überfordern“, „Ich habe zu große Bedenken oder Sorgen um meine Daten“ und „Ich habe Angst vor negativen sozialen Erfahrungen“.

¹⁵ Den Teilnehmenden wurden hierzu als Beispiele Identitätsdiebstahl, Datenmissbrauch oder Datenverlust genannt.

¹⁶ Als Beispiel wurden hierzu Übergriffe, Gewalt, Rassismus oder Diskriminierung genannt.

menden, die keine Zeit im Metaverse verbringen wollen, nannte lediglich ein knappes Datenschutzbedenken als Grund, der ihrer Nutzung eines Metaverse entgegensteht. Die Gründe für die geringe Relevanz von Datenschutzbedenken lassen sich bisher nur mutmaßen:

Zum einem ist denkbar, dass die Ähnlichkeit von Metaverse-Anwendungen zu Videospielen und anderen Unterhaltungsmedien das Thema Datenschutz in den Hintergrund treten lässt und die allgemeine Datenschutzrelevanz bei der Metaverse-Nutzung falsch eingeschätzt wird. Bereits im Rahmen der allgemeinen Internetnutzung haben betroffene Personen teilweise Schwierigkeiten, ihre Handlungen als personenbezogen einzuordnen.¹⁷ So könnte auch von der Metaverse-Nutzung angenommen werden, dass diese (zumindest gegenüber weiteren Nutzern) anonym ist.¹⁸ In einer Studie des Bitkom e. V. gaben immerhin zwei Drittel der Befragten an, es sei im Metaverse „noch schwieriger [...] herauszufinden mit wem man es tatsächlich zu tun hat.“¹⁹ Zwar ist es korrekt, dass Nutzer eines Metaverse untereinander in der Regel nicht ohne weiteres in der Lage sind, die Identität ihres Gegenübers zu bestimmen, das gilt allerdings nur, wenn pseudonyme Nutzernamen verwendet werden und auch der Avatar (in Kombination mit dem Namen) keine Identifizierungsmöglichkeit bietet. Eine vollständig anonyme Nutzung eines Metaverse gilt jedoch u. a. aufgrund potenzieller Haftungsfragen, Cyberkriminalität und Vertragsschlüssen – etwa beim Kauf von virtuellen oder physischen Gegenständen – als Herausforderung und lässt sich Experten nach nicht umsetzen.²⁰

Zum anderen könnten potenzielle Nutzer nicht ausreichend über Informationen zu Datenschutzrisiken verfügen oder solche unterschätzen. Zu diesen Risiken²¹ zählen insbesondere:

- Identitätsdiebstahl,²²
- Kommerzielle Zweckentfremdungen personenbezogener Daten und Überwachungen²³ sowie
- unzureichende Gewährleistungen der Betroffenenrechte.²⁴

Um feststellen zu können, ob sich Metaverse-Anwendungen zu einer Datenschutzfalle entwickeln könnten, müssen jene Risiken analysiert und in Verhältnismäßigkeit zu anderen Technologien gesetzt werden. Nach einer Erläuterung von Faktoren, die nach der DSGVO die Höhe eines Risikos beeinflussen, soll im Anschluss abstrahiert analysiert werden, wie ausgeprägt diese Faktoren bei Metaverse-Anwendungen sind, um die Risiken abschließend bewerten zu können.

4.1 Risikofaktoren nach der DSGVO

Nach Art. 24, 25 und 32 DSGVO lassen sich Risiken aus der Eintrittswahrscheinlichkeit sowie der Schwere der Risiken bzw. der hieraus resultierenden Schäden²⁵ im Rahmen einer Risikoanalyse bestimmen. Ziel des Vorgehens ist, im Anschluss angemessene technische und organisatorische Maßnahmen festlegen zu können, die die Risiken präventiv oder kurativ mindern oder beseitigen.²⁶ Faktoren, welche die Schadensschwere und die Eintrittswahrscheinlichkeit beeinflussen können, sind nach Art. 24, 25 und 32 DSGVO der Art, der Umfang, die Umstände und die Zwecke der Verarbeitung:

- Zwecke der Verarbeitungen können z. B. technische Anforderungen oder Analysen sein. Oftmals bestimmen sie zugleich die Art und besonders den Umfang der Verarbeitung. So dürfen personenbezogene Daten mit einem hohen Schutzwert etwa nur für bestimmte Zwecke verarbeitet werden.²⁷
- Die Art der Verarbeitung meint den jeweiligen, in Art. 4 Nr. 2 DSGVO genannten Vorgang (z. B. Erhebung oder Löschung personenbezogener Daten) sowie die Ausgestaltung als (teilweise) automatisierte oder manuelle Verarbeitung.²⁸ Nach der Konkretisierung der DSK ist davon auszugehen, dass vor allem automatisierte Entscheidungsfindungen i. S. d. Art. 22 DSGVO mit erheblichen Rechtswirkungen auf betroffene Personen als besondere Verarbeitungsform das Risiko erhöhen, z. B. die Bewertung persönlicher Aspekte (Profiling).²⁹
- Der Umfang einer Verarbeitung bezieht sich auf die Kategorien und die Anzahl betroffener Personen sowie personenbezogener Datenarten. So gehen nach Erwgr. 75 DSGVO Risiken „insbesondere“ aus einer Verarbeitung hervor, die eine „große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen“ zum Gegenstand hat. Nach der DSK kann auch eine breite, geographische Abdeckung das Risiko erhöhen, ebenso das Vorliegen von Daten besonders schützenswerter Personengruppen wie Kinder oder Beschäftigte.³⁰ Gleichermaßen können auch besonders schützenswerte Daten Risiken erhöhen, u. a. Daten besonderer Kategorien nach Art. 9 DSGVO sowie Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO,³¹ deren unbefugte Erlangung oder ungewollter Verlust besondere Eingriffe in die Privatsphäre der betroffenen Personen bedeuten. Das Vorhandensein vieler (sensibler) Daten kann Cyberangriffe zudem reizvoller werden lassen.³²
- Umstände der Verarbeitung umfassen wiederum Aspekte wie Ort und Dauer der Verarbeitung oder die Anzahl beteiligter Stellen.³³ Auch zur Verarbeitung verwendete Technolo-

17 Zur Datenverarbeitung und Anonymität aus der Sicht von betroffenen Personen Stummer/Hähle, DuD 2024, 800, 802.

18 Wenzel/Manca/Braun (Fraunhofer IAO), Regulierung des Metaversums, Stuttgart 2024, <https://publica-rest.fraunhofer.de/server/api/core/bitstream/ams/97ad1e7e-a974-4cff-8598-77b523c6930e/content>, S. 34.

19 Bitkom e. V., Erstmals kennt die Mehrheit das Metaverse, Berlin 2024, <https://www.bitkom.org/Presse/Presseinformation/Erstmals-kennt-Mehrheit-Metaverse>.

20 Fraunhofer IAO (Fn. 18), S. 15.

21 Um zwischen Risiken und Schäden unterscheiden zu können, die Risiken insgesamt benennen zu können, beziehen sich die Bezeichnungen hier auf die Schadensereignisse.

22 Interpol, Metaverse – A Law Enforcement Perspective, Januar 2024, <https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf>, S. 14.

23 Martini/Botta, MMR 2023, 887, 890 ff., welche vor „gläsernen Nutzern“ warnen.

24 Basierend auf Herausforderungen bzgl. der Informationspflichten und Löschung, s. Klar/Wegmann/Galandi, BB 2022, 2691, 2694 f.; Bender-Paukens/Werry, ZD 2023, 127, 129 f.

25 s. zur Konkretisierung aufgrund der „terminologische[n] Schwäche“ Lang, in: Taeger/Gabel, DSGVO BDSG TTDG, Art. 24 Rn. 37; m. V. a. Martini, in: Paal/Pau-ly, DS-GVO BDSG, Art. 24, Rn. 29.

26 Lang: in Taeger/Gabel, DSGVO BDSG TTDG, Art. 24, Rn. 39.

27 Ebenda, Rn. 47.

28 Ebenda, Rn. 43.

29 DSK, Kurzpapier Nr. 18, 26.04.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, S. 5.

30 Ebenda.

31 Vgl. Hartung, in: Kühling/Buchner, DSGVO, Art. 24, Rn. 14; a. A. Kipker, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, Art. 24 DSGVO, Rn. 21, wonach die Kategorien personenbezogener Daten zum Faktor „Art“ der Verarbeitung gehören.

32 Martini/Botta, MMR 2023, 887, 897.

33 Lang: in Taeger/Gabel, DSGVO BDSG TTDG, Art. 24, Rn. 46.

gien oder Systeme³⁴ beeinflussen das Risiko einer Verarbeitung, z. B. Anfälligkeiten für technische Fehlfunktionen oder wenn Aussparungen durch Dritte möglich sind.³⁵

4.2 Risikofaktoren im Metaverse

Bevor die Faktoren nun auf die zuvor dargestellten Risiken der Metaverse-Nutzung angewendet werden, soll eine abstrahierte Anwendung auf die grundsätzliche Metaverse-Nutzung erfolgen, um anschließend auf die Faktoren zurückverweisen zu können.

- Einige, aber nicht alle Zwecke der Datenverarbeitungen in Metaversen sind erforderlich, um ihre Funktionen bereitstellen zu können. Einige Zwecke können allein dem Anbieter von Metaverse-Anwendungen dienen, die sie als Verantwortliche selbst festlegen. So können z. B. Nutzeranalysen – wie auch bei der Internetnutzung – für diese finanziell attraktiv sein. Je mehr Daten über Nutzer vorliegen (s. u. zum Umfang), desto eher eignen sie sich auch zur Weiterverwendung für kommerzielle Zwecke wie Profiling.³⁶ Auch ist vorgesehen, dass Drittunternehmen oder Organisationen wie Krankenkassen innerhalb eines Metaverse „auftreten“ oder daran angebunden werden können, um personenbezogene Daten für eigene Zwecke zu nutzen.³⁷ Auch durch ihr Interesse an solchen Zwecken steigt die Wahrscheinlichkeit für solche Nutzungen.
- Die Arten der Verarbeitungen in Metaversen werden ebenfalls umfangreich sein, da personenbezogene Daten nicht nur erhoben und abgefragt, sondern (regelmäßig) auch gelöscht, übermittelt oder berichtigt werden müssen. Ist ein Metaverse zudem persistent³⁸ ausgestaltet, werden auch „alltägliche Handlungen“ teilweise – anders als im analogen Leben – nicht kurzfristig erhoben, sondern langfristig gespeichert, um die Einflüsse dauerhaft technisch umsetzen zu können und auch für andere Nutzer sichtbar zu machen. Diese und weitere Verarbeitungen erfolgen überwiegend automatisiert durch Systeme. Kommt es zu den zuvor genannten Analysezielen, erfolgen auch automatisierte Entscheidungsfindungen wie Profiling als besondere, riskantere Verarbeitungsarten.
- Bezüglich des Umfangs der Verarbeitung ist zunächst die Anzahl betroffener Personen in Metaversen erhöht, da diese in der Regel international verfügbar sind³⁹ und sich durch eine Vielzahl von Nutzern auszeichnen. Dabei kann es sich gleichzeitig – je nach Metaverse – um besonders schützenswerte Personengruppen handeln.⁴⁰ Die hohen Nutzerzahlen führen weiterhin – neben der Art und den Zwecken – zu einer erhöhten Anzahl verarbeiteter personenbezogener Daten,⁴¹ aus denen sich durch Analysen zusätzlich ggf. Rückschlüsse auf besonders schützenswerte ziehen lassen, z. B. die politische Meinung als

Datum besonderer Kategorien nach Art. 9 DSGVO.⁴² Ein Einsatz von VR-Zubehör führt dazu, dass regelmäßig biometrische Daten oder Gesundheitsdaten als weitere besondere personenbezogene Daten erfasst werden.⁴³

- Als risikoe erhöhende Umstände kommen hinzu, dass zum einem eine große Zahl von Unternehmen an Verarbeitungen im Metaverse beteiligt sind. Es kommt somit zu vermehrten Datenflüssen,⁴⁴ was die Anzahl an Datenweitergaben und die Gefahr von Zweckentfremdungen steigen lassen kann. Zum anderen werden in Metaverse-Anwendungen auch neue Technologien genutzt, die unterschiedliche Risiken bergen können, wie etwa künstliche Intelligenz.⁴⁵

4.3 Risikobewertung

Eine abstrahierte Anwendung der vier Faktoren auf die Metaverse-Nutzung zeigt folglich, dass Anhaltspunkte für erhöhte Risiken bestehen. Es stellt sich abschließend die Frage, wie sie sich auf die Eintrittswahrscheinlichkeit und die Schadensschwere der drei zuvor genannten Risiken auswirken. Dabei ist grundsätzlich zu beachten, dass sowohl Maßnahmen der Metaverse-Anbieter als auch das Verhalten der Nutzer die Eintrittswahrscheinlichkeit beeinflussen können, die hier außen vorgelassen wird.

Identitätsdiebstahl

Die Wahrscheinlichkeit für Identitätsdiebstähle dürfte in Metaversen durch die Umstände bzw. Einsatzmöglichkeiten von KI und Deepfakes als Täuschungsmittel⁴⁶ erhöht sein. Zusätzlich können die kommerziellen Komponenten eines Metaverse bzw. die Zwecke der Verarbeitungen den Anreiz erhöhen,⁴⁷ was (ohne entsprechende Maßnahmen) zu einer mindestens substanziellen Eintrittswahrscheinlichkeit führt. Wesentliche Folge eines Identitätsdiebstahls kann die Rufschädigung als immaterieller, gesellschaftlicher Schaden sein, welcher zugleich einen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO begründen kann.⁴⁸ Daneben können betroffene Personen aber auch erhebliche finanzielle Schäden erleiden, z. B. durch unautorisierte Käufe. Insgesamt ist daher von einer hohen Schadensschwere auszugehen.

Zweckentfremdungen und Überwachung

Besonders der Umfang der Verarbeitungen in Metaversen erhöht – im Vergleich zur Internetnutzung – die Attraktivität und damit auch die Wahrscheinlichkeit für die Durchführung von Nutzeranalysen und Profiling.⁴⁹ Auch die oben genannten Umstände bieten vermehrt Anlass für kommerzielle Zweckentfremdungen

34 Kipker, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, Art. 24 DSGVO, Rn. 21; a. A. Lang, in: Taeger/Gabel, DSGVO BDSG TDSG, Art. 24, Rn. 43, wonach die „Übertragungstechnik“ oder „Speichermedien“ der Art der Verarbeitung zuzuordnen wären.

35 DSK, Kurzpapier Nr. 18 (Fn. 29), S. 5

36 Klar/Wegmann/Galandi, BB 2022, 2691, 2693.

37 S. Geissler, Datenschutzrechtliche Rollen in Metaversen und im virtuellen Weiterleben, GI Informatik 2023, 497, 501 ff.

38 S. zur Persistenz Fn. 4

39 Fraunhofer IAO, (Fn. 18), S. 17.

40 Z. B. Roblox (s. Fn. 12), das überwiegend von Minderjährigen genutzt wird.

41 Maciejewski (Policy Department for Citizens' Rights and Constitutional Affairs European Parliament), Metaverse. Study Requested by the JURI Committee, Juni 2023, [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU\(2023\)751222_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf), S. 18

42 Martini/Botta, MMR 2023, 887, 894.

43 Das VR-Headset „Meta Quest“ von Meta verarbeitet nach ihren Datenschutzrichtlinien regelmäßig „Informationen zu körperlichen Merkmalen und Bewegungen“ und bietet Funktionen wie Hand- und Body-Tracking, Eye-Tracking und „natürliche Gesichtsausdrücke“ s. Meta, <https://www.meta.com/de/legal/quest/legal-bases/?srsltid=AfmBOorO8RfHImATFigeAgkoiaZIU5M-1YUN6tVtjJskyCXY5PBcnfR>, abgerufen am 28.1.2025; s. auch Gaff, in: Specht-Riemenschneider/Werry/Werry, Datenrecht in der Digitalisierung, § 2.3, Rn. 14.

44 Kaulartz/Schmid/Müller-Eising, RDI 2022, 521, 527 sprechen von einer „1-zu-X-Beziehung“ in der „virtuellen Fußgängerzone“.

45 Martini/Botta, MMR 2023, 887, 893 ff.

46 Ebenda, 895.

47 Robinson (GSMA), Exploring the metaverse and the digital future Februar 2022, <https://www.gsma.com/about-us/regions/asia-pacific/wp-content/uploads/2022/02/270222-Exploring-the-metaverse-and-the-digital-future.pdf>, S. 22.

48 EuGH, Urt. v. 20.6.2024 – C-182/22 und C-189/22, ZD 2024, 515.

49 Robinson, (Fn. 47), S. 22.

und Überwachungen der Nutzer.⁵⁰ Ohne Berücksichtigung möglicher Maßnahmen ist die Wahrscheinlichkeit als substantiell bis hoch zu bewerten. In Hinblick auf die Schadensschwere ist zu beachten, dass nach Ansicht der DSK ein Profiling – neben Einschränkungen der informationellen Selbstbestimmung und Kontrolle der betroffenen Personen – bereits einen eigenen Schaden darstellt.⁵¹ Umfang und Zwecke der Verarbeitungen, wie Analysen und die Verwendung sensibler Daten, können zugleich Eingriffe in die Privatsphäre darstellen sowie Diskriminierungsmöglichkeiten schaffen, weshalb hier die Schadensschwere als hoch betrachtet werden muss.

Unzureichende Gewährleistungen der Betroffenenrechte

Eng mit dem Risiko der Zweckentfremdung verknüpft ist bei der Metaverse-Nutzung zuletzt eine unzureichende Gewährleistung der Betroffenenrechte nach Art. 12 ff. DSGVO. Eine substantielle Wahrscheinlichkeit hierfür ergibt sich besonders durch mangelnde Datenschutzinformationen i. S. d. Art. 13 DSGVO, die entweder bewusst intransparent ausgestaltet bzw. unterdrückt werden, oder durch Herausforderungen bei der Umsetzung, welche sich aus den spezifischen Umständen und den Umfang der Verarbeitungen (s. o.) ergeben. Auch Komplikationen bei der Datenpflege bzw. Löschung nach Art. 17 DSGVO und Berichtigungen nach Art. 16 DSGVO sind durch die obigen Umstände wahrscheinlicher, insbesondere bei Verwendung der Blockchain-Technologie.⁵² Un-

⁵⁰ Denkbar sind im Arbeitskontext auch Arbeitnehmerüberwachungen, s. *Martini/Botta*, MMR 2023, 887, 890 f.

⁵¹ DSK, Kurzpapier Nr. 18 (Fn. 27), S. 3.

⁵² S. *Martini/Botta*, MMR 2023, 887, 889 zur Speicherung identifizierender Daten auf der Blockchain; Metaverse-Anbieter lassen angebundene Unternehmen zudem teilweise selbst entscheiden, welche Daten auf der Blockchain und welche auf regulären Servern gespeichert werden sollen, s. *Decentraland*, Docs:

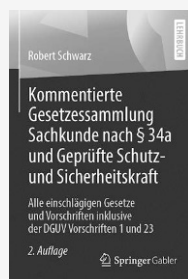
zureichende Gewährleistungen der Betroffenenrechte haben sowohl intransparente Verarbeitungen und damit Erschwerungen und Einschränkungen der Rechtsausübung zur Folge als auch eine Verhinderung der Kontrolle durch betroffene Personen. Diese Schäden können als substantielle Schäden eingeordnet werden.

5 Fazit und Ausblick

Die hier dargestellten, in der Literatur bereits angeführten Risiken der Metaverse-Nutzung sind aufgrund der Risikofaktoren im Hinblick auf ihre Eintrittswahrscheinlichkeit sowie Schadensschwere substantiell bis hoch. Gleichzeitig sind Datenschutzbedenken – zumindest nach der hier dargestellten Online-Umfrage – wiederum oft kein absoluter Hinderungsgrund für eine Nutzung, was nahelegen könnte, dass bestehende Datenschutzrisiken von potenziellen Nutzern unterschätzt werden. Metaverse-Anwendungen bergen folglich das Risiko, zu einer Datenschutzfalle zu werden. Ob dies jedoch tatsächlich eintritt, ist – je nach Risiko – einerseits von den zu ergreifenden Maßnahmen der Metaverse-Anbieter und andererseits den Nutzern selbst abhängig.

Die Nutzung neuer Technologien sollte aber nicht durch Ängste behindert werden. Stattdessen müssen die Rechte und Freiheiten der Nutzer als betroffene Personen in den Mittelpunkt gestellt werden, was in erster Linie transparente Informationen voraussetzt, damit sie fundierte Entscheidungen bezüglich ihres Nutzungsverhaltens treffen können.

About the blockchain, 30.01.2025: "The developers of each scene must choose what information is worth storing on the blockchain, and what to store in a private server", <https://docs.decentraland.org/player/blockchain-integration/ethereum-essentials/>.



Datenschutz

R. Schwarz
Kommentierte Gesetzessammlung Sachkunde nach § 34a und Geprüfte Schutz- und Sicherheitskraft

Alle einschlägigen Gesetze und Vorschriften
inklusive der DGUV Vorschriften 1 und 23

2. Aufl. 2019, aktualisierte, XI, 227 S. 1 Abb. Brosch.

€ (D) 14,99 | € (A) 15,41 | *sFr 17,00

ISBN 978-3-658-24546-7

€ 9,99 | *sFr 13,50

ISBN 978-3-658-24546-7 (eBook)

Ihre Vorteile in unserem Online Shop:

Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar |
Kostenloser Versand für Printbücher weltweit

Jetzt bestellen auf springer.com/DGUV1 oder in der Buchhandlung

Part of **SPRINGER NATURE**