Datenschutzrechtliche Rollen in Metaversen und im virtuellen Weiterleben

Von betroffenen Personen über Auftragsverarbeiter zu Verantwortlichen

Ines Geissler[1]

Abstract: Das Metaverse und Umgebungen des virtuellen Weiterlebens bieten großes Potenzial der Datenökonomie für Unternehmen und auch Menschen nutzen die virtuellen Welten immer mehr, um mit anderen Personen zu interagieren oder um mit Verstorbenen „in Kontakt" zu bleiben. Dadurch können eine Vielzahl an Akteuren an personenbezogenen Datenverarbeitungen beteiligt sein. Dieses Papier beschäftigt sich mit den datenschutzrechtlichen Verantwortlichkeiten und Rollen der Akteure im Metaverse und in Anwendungen des virtuellen Weiterlebens und diskutiert, ob KI-basierte Avatare mit einer eigenen Rechtspersönlichkeit ausgestattet werden sollten.

Keywords: Auftragsverarbeiter, Betroffene Personen, Datenschutz, Datenschutz-Grundverordnung, Virtuelles Weiterleben, Metaverse, Verantwortlichkeit.

1 Ein Einblick in zukünftige Formen des Lebens

1.1 Metaversen und Anwendungen des virtuellen Weiterlebens

Metaversen sind Räume des Internets, in der die virtuelle und analoge Realität miteinander verschmelzen. In diesen Räumen ist es Nutzern möglich, sich mit ihrer virtuellen Identität (in Form eines Avatars) zu bewegen und mit anderen Nutzern oder mit Organisationen zu interagieren, virtuelle Produkte zu erwerben oder virtuelle Dienstleistungen in Anspruch zu nehmen [Su22].

Anwendungen des virtuellen Weiterlebens ermöglichen dagegen das „Weiterleben" einer Person nach deren Tod (nachfolgend „Avatar-Inspirator"), i. d. R. in Form eines Avatars. Der Avatar-Inspirator lernt hierfür einen KI-basierten Avatar zu Lebzeiten an, so dass er durch diesen nach seinem eigenen Tod weiterleben kann, seine Angehörigen (nachfolgend „Hinterbliebene") weiter mit ihm interagieren können und so Unterstützung bei dem Trauerprozess oder bei alltäglichen Entscheidungen erhalten können [SM20].[2]

[1] Fraunhofer-Institut für Sicherer Informationstechnologie SIT | ATHENE – Nationales Forschungszentrum für angewandte Cybersicherheit, IT Law & Interdisciplinary Privacy Research, Rheinstr. 75, 64295 Darmstadt, ines.geissler@sit.fraunhofer.de, https://orcid.org/0009-0001-3416-6768.

[2] Das virtuelle Weiterleben findet nicht in Metaversen statt. Dies ist perspektivisch denkbar, im Folgenden werden Metaversen und Anwendungen des virtuellen Weiterlebens jedoch getrennt betrachtet.

In beiden Formen des virtuellen (Weiter-)Lebens werden eine Vielzahl personenbezogener Daten verarbeitet, in Metaversen insbesondere die personenbezogenen Daten der menschlichen Nutzer, in Umgebungen des virtuellen Weiterlebens u.a. die personenbezogenen Daten des Avatar-Inspirators und der Kommunikationspartner des weiterlebenden Avatars.

Insofern sind am virtuellen (Weiter-)Leben eine Vielzahl an Akteuren beteiligt, die es zu identifizieren und deren datenschutzrechtliche Rolle zu bestimmen gilt. Damit beschäftigt sich der nachfolgende Beitrag.

1.2 Datenschutzrechtliche Rollen aus der DSGVO

Das Datenschutzrecht kennt verschiedene datenschutzrechtliche Rollen der an einer Verarbeitung personenbezogener Daten Beteiligten. So unterscheidet es unter anderem zwischen dem Verantwortlichen, dem Auftragsverarbeiter und der betroffenen Person.

Verantwortliche sind gem. Art. 4 Nr. 7 DSGVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden.

Auftragsverarbeiter sind gem. Art. 4 Nr. 8 DSGVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

Betroffene Personen sind gem. Art. 4 Nr. 1 DSGVO natürliche Personen, deren personenbezogene Daten verarbeitet werden. Der betroffenen Person kommt in der DSGVO die wohl zentralste Rolle zu. Diese werden durch die DSGVO im Zusammenhang mit den sie betreffenden Daten vor unrechtmäßigen Eingriffen in ihre Rechte und Freiheiten geschützt.

Je nachdem welche Rolle den einzelnen Akteuren zugeordnet wird, entstehen für sie verschiedene datenschutzrechtliche Rechte und Pflichten, wie bspw.

- das Recht auf Information, Widerruf einer Einwilligung und Recht auf Löschung (betroffene Personen),
- die Pflicht zur Identifizierung und Umsetzung einer Rechtsgrundlage vor Datenerhebung, die Pflicht zum Schließen eines Auftragsverarbeitungsvertrags und die Pflicht zur umfangreichen Datenschutzdokumentation (Verantwortlicher bzw. gemeinsam Verantwortliche) und
- die Pflicht zum Ergreifen technischer und organisatorischer Maßnahmen, das Schließen eines Auftragsverarbeitungsvertrags und die Pflicht zur Beachtung der Weisungsrechte des Verantwortlichen (Auftragsverarbeiter).

Vor diesem Hintergrund ist es die Grundvoraussetzung eines datenschutzkonformen Agierens in Metaversen und im virtuellen Weiterleben, die datenschutzrechtlichen Rollen der beteiligten Akteure zu definieren.

2 Datenschutzrechtliche Rollen des virtuellen Lebens im Metaverse

Zu den Akteuren in Metaversen gehören unter anderem der Metaverse-Anbieter („Plattformanbieter"), menschliche Metaverse-Nutzer (die im Metaverse durch Avatare abgebildet werden), Unternehmen als Metaverse-Nutzer, Anbieter von technischen Dienstleistungen im Metaverse sowie Stellen, die in einem Metaverse Daten erheben wollen (wie z. B. Strafverfolgungsbehörden). Diese können umfangreich personenbezogene Daten bereitstellen, verarbeiten und miteinander austauschen.

2.1 Plattformanbieter

Ein Plattformanbieter stellt die Infrastruktur und Technologie bereit, die es den Nutzern ermöglicht, in der virtuellen Welt zu agieren. Dazu gehören beispielsweise die Server, die die Verbindung zwischen den Nutzern aufrechterhalten, die Software, die für die Erstellung und Verwaltung von Avataren verwendet wird, sowie die Schnittstellen, über die die Nutzer mit dem Metaverse interagieren können [Bo22].

In einem zentral strukturiertem Metaverse kommt dem Plattformanbieter die Rolle des datenschutzrechtlich Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO zu.

Der Plattformanbieter entscheidet sowohl über die Zwecke als auch über die Mittel der Datenverarbeitung [KSM22], z. B. darüber, welche Daten zur Registrierung erforderlich sind, welche Funktionalitäten die Plattform enthalten kann und mit welchen Schutzmaßnahmen den Risiken für die Rechte und Freiheiten der betroffenen Personen begegnet wird [Bi22].

Für Teile seines Metaverse-Angebots könnte der Plattformanbieter jedoch mit anderen Stellen gemeinsam verantwortlich sein (s. u.).

2.2 Organisationen als Nutzer

Auch Organisationen können Metaversen nutzen, indem sie sich als Unternehmen oder ihre Marke(n) und Produkte repräsentieren. So können etwa Events in Metaversen organisiert [Su22] sowie virtuelle Gegenstände zum Kauf angeboten werden [Bi22].

Diese Organisationen können dabei als datenschutzrechtlich Verantwortliche gem. Art. 4 Nr. 7 DSGVO handeln. Während der Nutzung von Metaversen verarbeiten diese Organisationen regelmäßig personenbezogene Daten der in den Metaversen agierenden Personen. Dazu gehören bspw. Anmeldedaten im Rahmen einer Anmeldung zu einem

Workshop. Für diese Datenverarbeitungen entscheiden sie über Zwecke und Mittel [BW23].

In Metaversen kann es allerdings auch vorkommen, dass mehrere Stellen an einer personenbezogenen Datenverarbeitung beteiligt sind. So ist es bspw. möglich, dass sich mehrere virtuelle Einzelhändler zu einem virtuellen Kaufhaus zusammenschließen [VAR12] und bspw. ein gemeinsames Treuepunktesystem anbieten. In diesem Fall entscheiden alle virtuellen Einzelhändler gemeinsam über die Zwecke und Mittel der Datenverarbeitung des Treuepunktsystems und sind somit hierfür gem. Art. 26 DSGVO gemeinsam verantwortlich, während sie für die sonstigen Datenverarbeitungen ihres Einzelhandels im Metaverse nicht mit den anderen Einzelhändlern gemeinsam verantwortlich sind.

Organisationen können als Nutzer jedoch auch eine gemeinsame datenschutzrechtliche Verantwortlichkeit mit dem Plattformanbieter eingehen.

Zwischen Organisationen als Nutzer sowie einem Plattformanbieter bestehen Parallelen zu dem Sozialen Netzwerk Facebook sowie den durch Organisationen betriebenen Facebook-Fanpages. Hierbei stellt Facebook die Plattform bereit und Organisationen können innerhalb der Plattform über ihre Fanpages eigene Dienste wie bspw. Umfragen, Marktanalysen oder Informationsaufbereitung anbieten. In diesem Zusammenhang werden Facebook weitere personenbezogene Daten der Nutzer bekannt, ohne dass die Betreiber der Fanpages dies beeinflussen können. Bei diesen Fanpages werden durch Facebook personenbezogene Daten der Fanpage-Besucher verarbeitet, während die Fanpage-Inhaber unter Umständen lediglich aggregierte Statistiken erhalten. Facebook-Fanpage-Inhaber sind laut einer EuGH-Entscheidung mit Facebook gemeinsam verantwortlich [Eu18].

In Metaversen ist dies ähnlich: Organisationen können als Nutzer ihre Dienste innerhalb der Metaverseplattform anbieten [Bi22]. So ist jeder virtuelle Einzelhändler wie eine Fanpage zu betrachten, durch den es dem Plattformanbieter ermöglicht wird, mehr Informationen über die betroffenen Personen zu erhalten. Dieser Parallele folgend wird hier die Meinung vertreten, dass auch der Plattformanbieter gem. Art. 26 DSGVO gemeinsam mit den Organisationen datenschutzrechtlich verantwortlich ist.[3]

[3] Anders sehen dies: [BW23], die eine gemeinsame Verantwortlichkeit als unrealistisch ansehen, da eine gemeinsame Festlegung der Zwecke und Mittel bei der großen Vielzahl an nutzenden Organisationen praktisch schwer umsetzbar ist. Dies ist in der Sache zwar richtig, allerdings trifft dieser Umstand auch auf Facebook-Fanpage-Inhaber zu, so dass aufgrund der o. g. EuGH-Entscheidung Best-Practice-Lösungen gefunden werden mussten, um die rechtlichen Anforderungen an die gemeinsame Festlegung der Zwecke und Mittel umzusetzen. Facebook-Fanpage-Inhaber berufen sich regelmäßig darauf, dass die mit Facebook geschlossenen Nutzugsvereinbarungen einen Vertrag über die gemeinsame Verantwortlichkeit impliziert.

2.3 Organisationen als technische Dienstleister

In Metaversen gibt es eine Vielzahl technischer Dienstleister, die Unternehmen und Einzelpersonen unterstützen, um ihre virtuellen Präsenzen zu betreiben. Hierzu gehören unter anderem Hostingdienstleister, die beispielsweise dem Plattformanbieter Server bereitstellen, sowie Zahlungsanbieter, die Dienstleistungen anbieten, um Transaktionen innerhalb von Metaversen zu erleichtern, wie zum Beispiel den Kauf von virtuellen Gütern [Bi22].

Fraglich ist nun, ob es sich bei diesen Dienstleistern um Verantwortliche gem. Art. 4 Nr. 7 DSGVO oder Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO handelt. Dies hängt davon ab, wer die Entscheidung über die Mittel und Zwecke der Verarbeitung innehat. Dies hängt wiederum vom konkreten Einzelfall ab und ob der Dienstleister selbst über die Mittel und Zwecke der Verarbeitung entscheidet oder ob er weisungsgebunden entsprechend den Vorgaben des Verantwortlichen Daten verarbeitet [LWG21].

Hostingdienstleister verarbeiten Daten für die Zwecke des datenschutzrechtlich Verantwortlichen und sind lediglich der verlängerte Arm dessen. Dem steht auch nicht der Umstand entgegen, dass Hostingdienstleister i. d. R. in gewissem Umfang selbst über die zu treffenden technischen und organisatorischen Maßnahmen entscheiden. Denn sofern dem datenschutzrechtlich Verantwortlichen die grundlegenden Entscheidungen über die Mittel sowie alle Entscheidungen über die Zwecke der Verarbeitung vorbehalten sind, steht ein geringer Spielraum bei der Auswahl der Mittel der Datenverarbeitung durch den Hostingdienstleister einer Auftragsverarbeitung regelmäßig nicht entgegen [TG22]. Somit kommt Hostingdienstleistern im Metaverse die datenschutzrechtliche Rolle des Auftragsverarbeiters zu. Dagegen sind Zahlungsdienstleister regelmäßig keine Auftragsverarbeiter, sondern eigenständige Verantwortliche [Ba19, WB23], weil sie Daten zu eigenen Zwecken und unter Festlegung der Verarbeitungsmittel verarbeiten [WB23]. Zudem haben Plattformanbieter keine Weisungs- oder Einsichtsrechte in Bezug auf die vom Zahlungsdienstleister gespeicherten Daten [FHS19].

2.4 Organisationen als Datennutzer

Des Weiteren können Organisationen im Metaverse auftreten, um die dort zugänglichen Daten zu nutzen. Dies kann besonders interessant für Krankenkassen, Gesundheitsämter, Krankenhäuser und ähnliche Institutionen sein [At23], die Daten der Nutzer, die sie selbst z. B. über ihren aktuellen Gesundheitszustand und Symptome preisgeben, im Metaverse analysieren, um beispielsweise Pandemien vorherzusagen, Krankheitsverläufe zu untersuchen oder Versicherungsleistungen zu begünstigen oder zu verwehren.

Auch Datenzugriffe, -auswertungen und -verknüpfungen durch staatliche Stellen wie zum Beispiel Strafverfolgungsbehörden sind denkbar und werden zum Teil bereits vorbereitet [In22]. Strafverfolgungsbehörden könnten beispielsweise per Beobachtung von Avataren auffällige Verhaltensmuster erkennen und so Straftaten aufdecken oder gar verhindern.

Die vorgenannten Stellen erheben diese Daten i. d. R. zu eigenen Zwecken und mit von ihnen selbst gewählten Mitteln, so dass sie für derartige Datenverarbeitungen datenschutzrechtlich verantwortlich sind. Anders als bei Facebook-Fanpages entscheiden diese Organisationen selbst über die Zwecke und Mittel der Verarbeitung und nutzen das Metaverse lediglich als Datenerhebungsquelle. Die durch sie erfolgende Datenspeicherung und -auswertung erfolgt i. d. R außerhalb des jeweiligen Metaverses und der Plattformanbieter erhält somit keinen zusätzlichen Zugang zu personenbezogenen Daten. Eine gemeinsame Verantwortlichkeit mit dem Plattformanbieter besteht daher regelmäßig nicht.

2.5 Menschliche, über Avatare abgebildete Nutzer

Durch ihre Nutzung der Metaversen werden ihre personenbezogenen Daten verarbeitet, so zum Beispiel die IP-Adresse, Bewegungsdaten ihres Avatars oder Daten über ihr Kaufverhalten [Bo22]. Der menschliche Nutzer ist eine betroffene Person im Sinne des Art. 4 Nr. 1 DSGVO. Menschen können Metaversen nutzen, indem sie als Avatare eine virtuelle Umgebung betreten und dort agieren und mit anderen Nutzern interagieren. Sie können beispielsweise Videospiele spielen, virtuelle Konferenzen abhalten und virtuelle Produkte und Dienstleistungen kaufen oder nutzen [Bi22].

Ein Avatar im Metaverse fungiert regelmäßig als digitale Identität eines Rechtssubjekts. Rechtssubjekte können natürliche und juristische Personen sein. Sofern sie durch natürliche Personen eingesetzt werden, werden sie also einer natürlichen Person zugerechnet. Diese Avatare können äußerliche Merkmale ihrer Nutzer haben und mit anderen Avataren und Akteuren im Metaverse in Kontakt treten [Bo22]. Die Avatare hinterlassen bei Nutzung der Metaversen Spuren in diesen. Ihr Verhalten und ihre Eigenschaften können personenbezogene Daten ihrer Nutzer aufweisen [KSM22]. Betreten Avatare bspw. virtuelle Kaufhäuser, können Informationen darüber erhoben werden, wie lange sich der Avatar dort aufhält und wofür er sich interessiert. Dabei handelt es sich um personenbezogene Daten ihrer Nutzer.

Da der Avatar von einem menschlichen Nutzer gestaltet und in dem betreffenden Metaverse bewegt wird, handelt der Avatar nicht autonom und ist somit weder eine juristische noch eine natürliche Person. Insofern kann er (selbst) weder Verantwortlicher, Auftragsverarbeiter noch betroffene Person sein.

3 Datenschutzrechtliche Rollen des virtuellen Weiterlebens

Auch im Kontext des virtuellen Weiterlebens bedarf es einer Identifizierung und Analyse der datenschutzrechtlichen Rollen.

3.1 Dienstanbieter

Dienstanbieter des virtuellen Weiterlebens sind Organisationen, die es technisch ermöglichen, mit einem Avatar zu kommunizieren, der zu Lebzeiten des Avatar-Inspirators von diesem KI-basiert trainiert wurde und sich sehr ähnlich verhält, wie der Avatar-Inspirator selbst [SM20]. Der Dienstanbieter entscheidet über die Zwecke und Mittel der Verarbeitung und stellt die technischen Möglichkeiten bereit, um die personenbezogenen Daten zu speichern und die Interaktion mit dem Avatar zu ermöglichen und ist insofern datenschutzrechtlich Verantwortlicher. Zu den personenbezogenen Daten, die von den Dienstanbietern des virtuellen Weiterlebens verarbeitet werden, können Informationen wie Nutzernamen, E-Mail-Adressen und alle anderen Daten gehören, die der Avatar-Inspirator dem Dienstanbieter (gewöhnlich über eine von ihm betriebenen Plattform) zur Verfügung stellt, um seinen Avatar anzulernen, bzw. die im Rahmen der Kommunikation zwischen Avatar und den Hinterbliebenen entstehen.

3.2 Menschliche Nutzer

Die Dienste des virtuellen Weiterlebens werden von Menschen in Anspruch genommen, die entweder mit verstorbenen Angehörigen kommunizieren wollen oder in Vorbereitung auf das eigene Ableben den eigenen Avatar anlernen und trainieren wollen, damit dieser dann nach ihrem Tod mit den Hinterbliebenen kommunizieren kann [SM20].[4] Dabei ist unter anderem zu klären, ob eine bereits verstorbene Person eine datenschutzrechtliche Rolle einnehmen kann.

3.2.1 Person, die über einen Avatar abgebildet wird

Sofern personenbezogene Daten des noch lebenden Avatar-Inspirators durch den Dienstanbieter verarbeitet werden, handelt es sich eben diesem gegenüber um eine betroffene Person im Sinne des Art. 4 Nr. 1 DSGVO. Er kann im Rahmen der Kommunikation beispielsweise Namen, Hobbies, Beruf und persönliche Erinnerungen preisgegeben, die zum Anlernen der KI verarbeitet werden.

Im Zusammenhang damit, dass der Avatar-Inspirator persönlicher Erinnerungen zum Anlernen der KI benutzt, die sich auf seine Hinterbliebenen beziehen und die personenbezogenen Daten seiner Hinterbliebenen enthalten, stellt sich die Frage, ob der Avatar-Inspirator für diesen Teil der Datenverarbeitung selbst datenschutzrechtlich verantwortlich sein könnte. Jedoch ist dies – ausgehend von der Annahme, dass die Nutzung dieser Daten ausschließlich zu rein privaten bzw. familiären Zwecken erfolgt –

[4] Der Prozess des Anlernens kann entweder zum Zeitpunkt des Todes des Avatar-Inspirators abgeschlossen sein oder noch nach dem Tod bspw. durch die Kommunikation mit Hinterbliebenen fortgeführt werden. Die vorliegende Veröffentlichung schließt letztgenannten Fall ein.

regelmäßig zu verneinen, weil der Avatar-Inspirator für diesen Datenverarbeitungsschritt unter die Haushaltsausnahme der DSGVO fällt, so dass für ihn die DSGVO nicht anwendbar ist und er somit auch nicht datenschutzrechtlich verantwortlich ist.

Die DSGVO regelt ausschließlich den Schutz personenbezogener Daten lebender Personen. Insofern ist der Avatar-Inspirator zwar vor seinem Tod, aber nicht mehr nach seinem Tod eine betroffene Person im Sinne der DSGVO.

3.2.2 Kommunikationspartner des Avatars

Kommunikationspartner des Avatars zu Lebzeiten können beispielsweise Angehörige und Freunde sein, die dem weiterlebenden Avatar Informationen, über die ihn inspirierende Personen weitergeben wollen. In diesem Zusammenhang werden von dem Dienstanbieter (durch den von ihm betriebenen, KI-basierten Avatar) personenbezogene Daten dieser Personen verarbeitet. Die Kommunikationspartner des Avatars zu Lebzeiten des Avatar-Inspirators sind gegenüber dem Dienstanbieter betroffene Person im Sinne des Art. 4 Nr. 1 DSGVO. Zu den verarbeiteten Daten können neben der IP-Adresse auch Informationen über die persönliche Beziehung zum Avatar-Inspirator gehören. Die Avatare können während ihrer Interaktionen personenbezogene Daten über die Kommunikationspartner sammeln und zu Trainingszwecken der KI verwenden [SM20]. Darüber hinaus können die Nutzer dem Dienstanbieter personenbezogene Daten wie ihren Namen, ihre E-Mail-Adresse und andere Informationen zur Verfügung stellen, damit sie mit den KI-generierten Avataren interagieren können.

Auch die Kommunikationspartner des Avatars eines verstorbenen Avatar-Inspirators sind gegenüber dem Dienstanbieter betroffene Personen gem. Art. 4 Nr. 1 DSGVO, da bei einer Kommunikation ebenso personenbezogene Daten wie IP-Adressen und z. B. die dem Avatar gestellten Fragen verarbeitet werden.

3.3 Avatar

Schließlich stellt sich die Frage, ob der KI-basierte Avatar, mittels dessen eine real lebende Person durch ein entsprechendes Dienstleistungsangebot des Dienstanbieters nach dem Tod virtuell weiterleben kann, selbst eine datenschutzrechtliche (ggf. mit dem Dienstanbieter gemeinsame) Verantwortung trägt, weil der Avatar selbst möglicherweise gegen geltendes Datenschutzrecht verstoßen könnte, z. B. in dem personenbezogene Daten von Hinterbliebenen anderen Kommunikationspartnern ungewollt offengelegt werden. So könnte der Avatar bspw. den Verlust des Arbeitsplatzes, eine Schwangerschaft oder eine Scheidung eines seiner Kommunikationspartner verkünden. Aus derartigen Datenschutzverstößen könnten sich gegebenenfalls Haftungsansprüche ergeben. Fraglich ist in dem Zusammenhang, ob diese dem Avatar (als datenschutzrechtlich Mitverantwortlichem) selbst zuzuordnen sind.

Die Auffassung, dass KI-basierten Avataren eine datenschutzrechtliche (Mit-)Verantwortlichkeit zukommen könnte, stützt sich auf folgende Überlegungen:

1. (K)eine Entscheidungsfähigkeit über die Zwecke der Verarbeitung

Ein datenschutzrechtlich Verantwortlicher muss in der Lage sein, den Verarbeitungsprozess zu steuern [PP21]. Dies könnte auf das KI-System zutreffen, wenn das KI-System selbst entscheiden würde, ob und zu welchen Zwecken Daten gespeichert oder gelöscht werden. KI-Systeme mit niedrigem Autonomiegrad beziehen die von ihm verarbeiteten Daten regelmäßig aus einer Datenbank [Bl20], im Falle des virtuellen Weiterlebens i. d. R. aus einer Datenbank des Dienstanbieters, die er wiederum mit Daten des Avatar-Inspirators und seiner Kommunikationspartner befüllt bzw. von den Vorgenannten befüllen lässt, so dass der Dienstanbieter die Entscheidung trifft, auf welche Daten das KI-System zugreifen kann. Auch die Zwecke des Einsatzes des KI-Systems – und somit der Datenverarbeitung durch das KI-System – legt der Dienstanbieter fest. KI-Systeme mit hohem Autonomiegrad können dagegen selbst festlegen, welche personenbezogenen Daten sie zu welchem Zweck verarbeiten möchten [Bl20]. Grundsätzlich wird also bei KI mit niedrigem Autonomiegrad davon auszugehen sein, dass der Dienstanbieter allein verantwortlich ist. Bei hohem Autonomiegrad könnte eine eigene Entscheidungsfindung hinsichtlich des Zwecks der Verarbeitung getroffen werden, so dass theoretisch eine gemeinsame Verantwortlichkeit mit dem Dienstanbieter in Betracht käme. Da die KI aber weder juristische noch natürliche Person ist, müsste sie zu einem Rechtssubjekt mit Rechtspersönlichkeit gemacht werden, die in der Lage wäre, Rechte und Pflichten zu erfüllen und datenschutzrechtliche Verantwortung zu übernehmen.

2. Einführung einer ePerson in der aktuellen Diskussion

Die Frage nach der Verantwortlichkeit und der Zuordnung zum menschlichen Handeln ist bei dem Einsatz von KI nicht immer einfach zu definieren. Um mehr Klarheit zu schaffen, wird insbesondere im Haftungsrecht über die Einführung einer elektronischen Person (ePerson) diskutiert. Bisher werden ausschließlich natürliche und juristische Personen als Rechtssubjekt mit Rechtspersönlichkeit angesehen. Diese sind rechtsfähig [Ri20]. Die ePerson wäre vergleichbar mit einer juristischen Person, so dass ihr eine eigene Rechtspersönlichkeit zugeschrieben und sie damit Rechtsfähigkeit besitzen würde. Die KI würde dadurch Inhaberin von Rechten und Pflichten und in Schadensfällen selbst zu Verantwortung gezogen werden und damit selbst für ihr Handeln haften [WZ03]. Die Einführung der ePerson würde dazu führen, dass Schäden haftungsrechtlich klar zugeordnet werden könnten und Beweisprobleme vermieden würden [LWG21].

Für eine Einführung einer ePerson spricht auch, dass KI-Systeme, genau wie Menschen, sich an die Umwelteinflüsse anpassen und ohne menschliche Mitwirkung Entscheidungen treffen können [KM15]. Der technische Fortschritt könnte sogar dazu führen, dass KI-Systeme die gleichen Denkprozesse wie Menschen aufweisen. Diese Vergleichbarkeit der Denkprozesse würde bedeuten, dass auch vergleichbare Rechte und Pflichten bestehen müssten [Be09].

Diesen Überlegungen kann nach der hier vertretenen Meinung aus den folgenden Gründen jedoch nicht gefolgt werden:

a) Entscheidungen müssen auf natürliche Personen zurückgeführt werden können.

Grundsätzlich gilt, dass Entscheidungen über Zwecke und Mittel auf eine natürliche Person zurückgeführt werden müssen [HSH22]. Insbesondere bei der automatisierten Entscheidungsfindung inklusive Profiling muss sichergestellt werden, dass diese Entscheidung durch einen Menschen überprüft werden kann [WB23].

KI-Systeme können anfällig für Diskriminierungen sein, insbesondere dann, wenn sie auf nicht repräsentativen Datensätzen trainiert werden. Insofern sollten wichtige Entscheidungen nicht von KI-Systemen übernommen werden [Dj22].

b) Eine eigene Verantwortlichkeit durch Gesetzgeber wird nicht vorgesehen.

Zwar hatte das EU-Parlament 2017 vorgeschlagen „langfristig einen speziellen rechtlichen Status für Roboter zu schaffen, damit zumindest für die ausgeklügelten autonomen Roboter ein Status als elektronische Person festgelegt werden könnte, die für den Ausgleich sämtlicher von ihr verursachten Schäden verantwortlich wäre […]“ [Eu17], dies wurde allerdings durch die EU-Kommission nicht aufgegriffen [Eu19].

Die EU plant im Rahmen des durch die EU-Kommission vorgelegten Vorschlags einer KI-Verordnung den Rechtsrahmen für künstliche Intelligenz zu regeln. Der KI-Verordnung-Entwurf verfolgt einen risikobasierten Ansatz, der Regulierungsstufen aufweist. So sollen bestimmte, besonders risikobehaftete KI-Anwendungen verboten werden und andere KI-Anwendungen bestimmte technische und organisatorische Vorgaben erfüllen und einer Konformitätsbewertung unterliegen [BM21]. Eine eigene Rechtspersönlichkeit für KI ist auch hier nicht vorgesehen.

Art. 52 KI-Verordnung-Entwurf besagt, dass KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden müssen, dass natürlichen Personen mitgeteilt wird, dass sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Weiterhin wird in Erwägungsgrund 53 der KI-Verordnung als angemessen empfunden, dass eine bestimmte als Anbieter definierte natürliche oder juristische Person die Verantwortung für das Inverkehrbringen oder die Inbetriebnahme von Hochrisiko-KI-System übernimmt.

c) Die KI wird nicht verkörpert.

Insbesondere in Bezug auf KI-basierte Avatare im virtuellen Weiterleben bestehen Probleme in Bezug auf die Verkörperung. Während autonome Fahrzeuge und physische Roboter körperlich identifiziert werden können und somit ein Rechtssubjekt darstellen könnten, ist eine derartige Identifizierung bei virtuellen Avataren u. U. nicht möglich. Wenn im Kontext des virtuellen Weiterlebens beispielsweise mehrere Avatare auf dem

gleichen Algorithmus basieren, ist unklar, wie viele Rechtspersönlichkeiten vorliegen [Ri20]. Für jeden Avatar eine eigene oder eine zentrale Rechtspersönlichkeit für alle Avatare, die auf dem gleichen Algorithmus basieren?

d) KI hat nicht die (finanzielle) Motivation, sich an Gesetze zu halten.

Gegen die Einführung der ePerson spricht außerdem, dass KI-Systeme keine Bedrohung beziehungsweise keinen Anreiz in der Anpassung ihres Verhaltens hinsichtlich der Haftung sehen. Diese Verhaltensanpassung erfolgt bei natürlichen Personen, weil sie Sanktionen vermeiden möchten und auch das Verhalten juristischer Personen wird aufgrund der Gewinnerzielungsabsicht gesteuert. Ein KI-System verfolgt keines dieser Interessen und hat somit auch kein Interesse daran, sich Rechtsordnungen anzupassen. Mögliche Haftungsmassen müssten über Beiträge aus möglichen Haftpflichtversicherungen gezahlt werden, so dass KI-Systeme mit einem Mindestkapital ausgestattet werden müssen. Dieses müsste wiederum von Hersteller oder Betreiber oder anderen Akteuren gezahlt werden [Ri20].

Folglich kommt dem Avatar nach hier vertretener Ansicht keine eigene datenschutzrechtliche Rolle zu und die Verantwortung für die durch den Avatar erfolgende personenbezogene Datenverarbeitung ist grundsätzlich (allein) dem Dienstanbieter zuzuschreiben.

4 Zusammenfassung und Ausblick

Grundvoraussetzung für ein rechtskonformes Handeln im Zusammenhang mit dem virtuellen Weiterleben und dem Leben im Metaverse ist, dass allen Beteiligten klar sein muss, welche datenschutzrechtlichen Rechte sie innehaben, und welche Rechte und Pflichten sie entsprechend ihrer datenschutzrechtlichen Rollen erfüllen müssen. Der vorliegende Beitrag konnte folgende Akteure und datenschutzrechtlichen Rollen identifizieren und zuweisen:

Akteur	**Datenschutzrechtliche Rolle**
Metaversen	
Plattformanbieter	Kontextabhängig alleinige oder gemeinsame Verantwortliche
Organisationen als Nutzer	Kontextabhängig alleinige oder gemeinsame Verantwortliche
Organisationen als technische Dienstleister	Kontextabhängig gemeinsam Verantwortliche oder Auftragsverarbeiter
Organisationen als Datennutzer	Alleinige Verantwortliche

Menschliche, über Avatare abgebildete Nutzer	Menschen: Betroffene Personen
	Avatare: Keine datenschutzrechtliche Rolle
Virtuelles Weiterleben	
Dienstanbieter	Verantwortliche
Menschliche Nutzer	Lebende Personen: Betroffene Personen
Avatar	Keine datenschutzrechtliche Rolle

Tab. 1: Akteure und ihre datenschutzrechtlichen Rollen

Im Zusammenhang mit der Analyse der datenschutzrechtlichen Verantwortlichkeit des Avatars wurde darüber hinaus diskutiert, ob ein Avatar mit einer eigenen Rechtspersönlichkeit ausgestattet werden sollte. Dies ist insbesondere wegen der fehlenden finanziellen Motivation, die natürliche und juristische Personen haben, um geltendes (Datenschutz-)Recht einzuhalten, zu verneinen.

Perspektivisch scheint die Rolle des Avatar-Inspirators des virtuellen Weiterlebens aus datenschutzrechtlicher Sicht von besonderer Bedeutung zu sein, da dieser nach seinem Ableben keinen direkten Einfluss mehr auf den Avatar und die damit verbundenen Verarbeitungsprozesse nehmen kann. Aber auch in Bezug auf potenzielle Verletzungen seines postmortalen Persönlichkeitsschutzes scheint die Rolle des Avatar-Inspirators vor diesem Hintergrund besonders bedeutungsvoll zu sein, so dass mögliche Risiken für diese Rolle Gegenstand zukünftiger vertiefter Forschung sein sollte.

Danksagung

Diese Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projektes „Edilife“ (Förderkennzeichen: 6INS114B) sowie vom Bundesministerium für Bildung und Forschung (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.

Literaturverzeichnis

[AAM23] Athar, A.; Ali, S. M.; Mozumder, M. A. I.; Ali, S.; Kim, H. - C.: "Applications and Possible Challenges of Healthcare Metaverse," 25th International Conference on Advanced Communication Technology (ICACT), S. 328-332, 2023.

[Be09] Beck, S.: Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR, S. 225-230, 2009.

[Bi22] Bitkom e.V.: Wegweiser in das Metaverse – Technologische und rechtliche Grundlagen, geschäftliche Potenziale, gesellschaftliche Bedeutung, 2022.

[Bl20] Bleckat, A.: Anwendbarkeit der Datenschutzgrundverordnung auf künstliche Intelligenz, DuD, S. 194-198, 2020.

[BM21] Bomhard, D.; Merkle, M.: Europäische KI-Verordnung, Rdi, S. 276-283, 2021.

[Bo22] Bossmann, O.: Das Metaverse – Schöne neue Zukunft oder Datenschutz-Albtraum, Neuss 2022.

[BW23] Bender-Paukens, L.; Werry, S.: Datenschutz im Metaverse, ZD, S. 127-131, 2023.

[Dj22] Djeffal, C.: „Soziale Medien und Kuratierung von Inhalten. Regulative Antworten auf eine demokratische Schlüsselfrage.“ In: Spiecker, I.: Demokratie und Öffentlichkeit im 21. Jahrhundert–zur Macht des Digitalen. Nomos Verlagsgesellschaft mbH & Co. KG, S. 177-189, 2022.

[Eu17] EU-Parlament, Entschließung vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik, 2017.

[Eu18] EuGH, Urteil vom 05.06.2018 – C-210/16.

[Eu19] EU-Kommission, Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz, COM, 2019.

[HSH22] Hoeren, T.; Sieber, U.; Holznagel, B.: Handbuch Multimediarecht, 4. Auflage, C. H. Beck, 2022.

[In22] Interpol Technology Assessment Report on the Metaverse, 2022.

[KM15] Kirn, S.; Müller-Hengstenberg, C.: Technische und rechtliche Betrachtungen zur Autonomie kooperativ-intelligenter Softwareagenten, Künstliche Intelligenz 29, S. 59–74, 2015.

[KSM22] Kaulartz, M.; Schmid, A.; Müller-Eising, F.: Das Metaverse – eine rechtliche Einführung, RDi 2022, S. 521-532.

[LWG21] Leupold, A.; Wiebe, A.; Glossner, S.: IT-Recht – Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage, C. H. Beck, 2021.

[Ri20] Riehm, T.: Nein zur ePerson!, Rdi, S. 42-48, 2020.

[SM20] Savin-Baden, M.; Mason-Robbie, V.: Digital Afterlife – Death Matters in a Digitale Age, CRC Press, 2020.

[Su22] Sury, U.: Metaverse – parallele Welt(en), Informatik Spektrum, S. 407-409, 2022.

[TG22] Taeger, J.; Gabel, D.: Kommentar DSGVO – BDSG – TTDSG, 4. Auflage, C. H. Beck, 2022.

[VAR12] Vernaza, A; Armuelles, V. I.; Ruiz, I.: "Towards to an open and interoperable virtual learning enviroment using Metaverse at University of Panama," Technologies Applied to Electronics Teaching, S. 320-325, 2012.

[WB23] Wolff, H. A.; Brink, S.: Beck’scher Online-Kommentar Datenschutzrecht, 43. Edition, C. H. Beck, 2023.

[WZ03] Wettig, S.; Zehendner, E.: The Electronic Agent: A Legal Personality under German Law?, https://beck-link.de/kc3tt, Stand: 15.05.2023.