Privacy by Design: Schutz der Privatheit im Metaverse durch Designpraktiken am Beispiel ausgewählter Gefahren für Datenschutz und Persönlichkeitsrechte

Tom Hubert, Felix Büning, Marwan El-Rifaai, Florian Franke, Michael Kern, Sara Elisa Kettner, Otmar Lell, Markus Meyer, Runjie Xie, Benedikt Morscheuser, Christian Thorun und Andreas Wiebe[*]

Zusammenfassung
Das Metaverse eröffnet neue Möglichkeiten für digitale Interaktionen, birgt jedoch zugleich erhebliche Herausforderungen für den Schutz von personenbezogenen Daten und Persönlichkeitsrechten. Ein zentraler Ansatz zur Bewältigung dieser Herausforderungen ist das Konzept des „Privacy by Design", bei dem Datenschutz- und Persönlichkeitsrechte bereits in der Entwicklung virtueller Umgebungen berücksichtigt werden. Dieser Beitrag untersucht verschiedene Designstrategien, die zur Wahrung der Privatheit im Metaverse beitragen können. Die Untersuchung zeigt, dass wirksame Schutzmaßnahmen vor allem dann erfolgreich sind, wenn sie technisch umsetzbar und für die Nutzer intuitiv verständlich sind. Gleichzeitig bestehen Herausforderungen bei der praktischen Implementierung dieser Maßnahmen, insbesondere im Hinblick auf die Balance zwischen Nutzerfreundlichkeit und Vereinbarkeit mit den rechtlichen Anforderungen, wie insbesondere dem Datenschutzrecht.

1. Einleitung

Das Metaverse (Metaversum) birgt gewaltiges ökonomisches Potenzial und könnte alle Bereiche unseres täglichen Lebens, unserer Kultur und Gesellschaft durchdringen.[1] Bis heute existiert das Metaverse noch nicht, doch es wird als eine nächste Stufe des Internets betrachtet, die es Nutzern ermöglicht, neue soziale und interaktive Erlebnisse zu erfahren, deren Spektrum

* Die Autoren arbeiten gemeinsam im Projekt PRIME – Privatheit im Metaversum, in dem fachübergreifend erforscht wird, wie neue virtuelle Welten mit Persönlichkeitsrechten und Datenschutz in Einklang gebracht werden können. Das Projekt ist Teil der Plattform Privatheit und wird durch das BMBF unter dem Förderkennzeichen 16KIS1894K gefördert. Der Beitrag verwendet zwecks Leserlichkeit das generische Maskulinum, gemeint sind jedoch alle Geschlechter und Identitäten.

1 S. etwa *Gartner*, Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026, 2022.

von einer digitalen Erweiterung unserer Realität bis hin zu vollständig virtuellen Welten reicht.[2]

Mit der zunehmenden Verschmelzung von physischer und digitaler Realität im Metaverse rücken Fragen des Datenschutzes und des Schutzes von Persönlichkeitsrechten in den Mittelpunkt der Forschung. Die Nutzung immersiver Technologien führt zu neuen Bedrohungsszenarien, die die Privatheit der Nutzer gefährden, beispielsweise durch besonders intensive Datenerfassung, Verhaltensanalysen oder manipulative Eingriffe.

Ein zentraler Ansatz zur Sicherung von Persönlichkeitsrechten und Datenschutz im Metaverse liegt im Privacy-by-Design-Ansatz, der die Grundprinzipien des Schutzes von Rechten direkt in die Gestaltung von Plattformen, digitalen Medieninhalten und Technologien integriert. Vor diesem Hintergrund stellt sich die Frage, wie Privacy-by-Design in die Gestaltung des Metaverse und seiner Inhalte einfließen kann, um Risiken wirksam zu minimieren und gleichzeitig eine praktikable Umsetzung dieser Lösungen sicherzustellen. Die bisherige Forschung ist jedoch noch in ihren Anfängen und eine integrierte Betrachtung der juristischen, technischen und gesellschaftlichen Aspekte mit Bezug zu sowohl dem Schutz der Persönlichkeitsrechte als auch dem Schutz personenbezogener Daten findet kaum statt.

Als Forschungsfrage sei daher formuliert: *Wie lassen sich wirksame Privacy-by-Design-Lösungen zum Schutz von Persönlichkeitsrechten und personenbezogener Daten im Metaverse entwickeln sowie implementieren und welche Herausforderungen ergeben sich dabei in Bezug auf die Realisierbarkeit aus Nutzerperspektive?*

2. Das Metaverse – Immersive Realitäten

Der Begriff Metaverse, geprägt durch Neal Stephensons Roman *Snow Crash*[3], setzt sich aus „Μετά“ (griechisch für „darüber hinaus“) und „-verse“ (Kurzform von „Universe“, bedeutet „Gesamtheit von etwas“) zusammen. Das Konzept ist vielschichtig und offen für Interpretationen.[4] Es umfasst ein breites Spektrum an Ansätzen, angefangen bei der digitalen Erweiterung der physischen Realität (d.h. Augmented Reality - AR) über vollständig virtuelle Welten (d.h. Virtual Reality - VR) bis hin zu virtuellen

2 *Accenture*, Meet Me in the Metaverse, 2022, S. 24.
3 *Stephenson*, Snow Crash, 1992.
4 *Dolata/Schwabe*, What is the Metaverse and who seeks to define it?, Journal of Information Technology 2023, 239.

Umgebungen, die wiederum durch reale Elemente ergänzt werden (z.B. augmentierte Virtualität - AV).

Experten betrachten das Metaverse als die nächste Entwicklungsstufe des Internets, die aus vernetzten persistenten 3D-Welten besteht, in denen Nutzer als Avatare auftreten und mit anderen Nutzern, virtuellen Objekten und KI-Agenten interagieren.[5] Ein zentrales Konzept des Metaverse ist die Interoperabilität, durch welche Nutzer nahtlos zwischen verschiedenen Welten wandeln können, während Identität und (virtueller) Besitz erhalten bleiben.[6] Ein weiterer wesentlicher Aspekt ist die Möglichkeit für Nutzer, nicht nur passiv zu konsumieren, sondern die virtuelle Welt aktiv mitzugestalten. Dabei können sie sich am Metaverse-Ökosystem beteiligen und zur Schaffung ökonomischer und sozialer Werte beitragen.[7]

Zentral für das Metaverse ist das Erleben von Präsenz, das subjektive Gefühl, tatsächlich in der virtuellen Welt anwesend zu sein.[8] Dieses Empfinden wird durch die wahrgenommene Immersion verstärkt, die durch einen kontinuierlichen Strom sensorischer Reize moderner Metaverse-Technologien, wie realistischer Grafik und räumlichem Sound, gezielt gefördert wird. Während das klassische Internet primär visuelle und auditive Sinneseindrücke anspricht, verfolgt das Metaverse die Vision, ein breiteres Spektrum an Sinneswahrnehmungen einzubeziehen. Einige dieser Reize sind derzeit noch nicht breit kommerziell verfügbar (z.B. Geruch oder Geschmack), andere hingegen, wie der Tastsinn durch haptische Technologien, der Gleichgewichtssinn durch simulierte Bewegungen oder die Propriozeption über präzises Körper-Tracking, werden bereits erfolgreich integriert. Dadurch entsteht eine Illusion realistischer Wahrnehmung, die die Grenzen zwischen Realität und Virtualität zunehmend auflöst.[9]

Ein vollständig durchgängiges Metaverse im idealen Sinne existiert heute noch nicht. Dennoch finden sich viele Grundideen des Metaverse bereits in bestehenden Technologien, etwa in Open-World-MMORPGs wie Second Life oder World of Warcraft, in sozialen Medien oder in cyberphysischen

5 *Davis u.a.*, Avatars, People, and Virtual Worlds, Journal of the Association for Information Systems 2009, 90.

6 *Dionisio u.a.*, 3D Virtual worlds and the metaverse, ACM Computing Surveys 2013, 34.

7 *Papagiannidis u.a.*, Making real money in virtual worlds, Technological Forecasting & Social Change 2008, 610.

8 *Witmer/Singer*, Measuring presence in virtual environments: A presence questionnaire, Presence: Teleoperators and Virtual Environments 1998, 225.

9 *Dincelli/Yayla*, Immersive virtual reality in the age of the Metaverse, The Journal of Strategic Information Systems 2022, 101717.

Systemen. Außerdem bieten viele Spieleentwickler bereits erste Proto-Metaverse-Plattformen an, die zahlreiche Merkmale des Metaverse gut abbilden, darunter Roblox, Fortnite und Minecraft.[10] Auch die Krypto- und NFT-Community hat ähnliche Ansätze geschaffen, wie beispielsweise Decentraland und The Sandbox.[11]

Das Metaverse könnte vielfältige Chancen für Unternehmen und die Gesellschaft bieten, wie zum Beispiel in den Bereichen Remote Work, Gesundheit und Bildung.[12] Gleichzeitig birgt es jedoch auch Schattenseiten, die das volle Potenzial des Metaverse hemmen können.[13] Diese Herausforderungen sind bereits auf den ersten Proto-Metaverse-Plattformen erkennbar und müssen frühzeitig angegangen werden, um die Grundlage für ein zukünftiges rechtskonformes Metaverse zu schaffen.

3. Risiken des Metaverse für die Privatheit

Unter den zahlreichen Herausforderungen des Metaverse ragt der Schutz der Privatsphäre als besonders problematisch hervor.[14] Privatheit ist ein multidimensionales Konzept, welches das Recht und die Fähigkeit umfasst, die eigene Person sowie persönliche Informationen, Gedanken und Handlungen vor dem Eingriff Dritter zu schützen.[15] Eine Verletzung der Privatheit greift sowohl die Persönlichkeitsrechte als auch die Datenschutzrechte der Nutzer an und kann zu erheblichen Beeinträchtigungen der individuellen Freiheit und Sicherheit führen.

10 *Schöbel/Leimeister*, Metaverse platform ecosystems, Electronic Markets 2023, 33 (12).
11 *Dolata/Schwabe*, What is the Metaverse and who seeks to define it? Mapping the site of social construction, Journal of Information Technology 2023, 38 (3).
12 *Marabelli/Newell*, Responsibly strategizing with the metaverse: Business implications and DEI opportunities and challenges, The Journal of Strategic Information Systems 2023, 101774.
13 *Dwivedi u.a.,* Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, International Journal of Information Management 2022, 102542; *Dwivedi u.a.,* Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse, Information Systems Frontiers 2023, 2071.
14 *Xie/Kirchner-Krath/Morschheuser*, Towards an Ethical Metaverse: A Systematic Literature Review on Privacy Challenges, Proceedings of the 32nd European Conference on Information Systems (ECIS) 2024,6.
15 *Zhang u.a.*, Peer Privacy Concerns: Conceptualization and Measurement, MIS Quarterly 2022, 46 (1).

3.1 Gefahren für Persönlichkeitsrechte

Ein zentraler Aspekt privatheitsbezogener Herausforderungen ist der Schutz von Persönlichkeitsrechten, die Selbstbestimmung und individuelle Freiheit gewährleisten sollen. Aus der Perspektive des deutschen Rechts treten im Kontext des Metaverse besondere Gefährdungen für den Persönlichkeitsschutz auf. Diese werden insbesondere durch virtuelle zwischenmenschliche Interaktionen und der Präsenz automatisierter Software-Agenten bedingt.

3.1.1 Virtuelle Belästigung

Trotz der vergleichsweise noch geringen Zahl an Nutzern in virtuellen Welten, gibt es bereits vermehrt Berichte von Menschen, die mit ihren Avataren Opfer von virtuellen Belästigungen geworden sind.[16] Der Begriff der Belästigung kann weit gefasst werden und umfasst hier jedenfalls jedes bewusste, unerwünschte virtuelle Verhalten, wie beispielsweise Berührungen, Ansprechen oder das Herbeiführen von Begegnungen im Metaverse. Solche Belästigungen erhalten durch die avatarbasierte Kommunikation eine neue Qualität, da sie nicht mehr „nur" text- oder sprachbasiert erfolgen, sondern insbesondere auch durch Gestik, Mimik und Körpersprache der jeweiligen Avatare vermittelt werden können.

Erste Untersuchungen deuten darauf hin, dass Belästigungen im Metaverse deutlich belastender wahrgenommen werden können als vergleichbare Ereignisse auf „herkömmlichen" zweidimensionalen Plattformen.[17] Dies liegt in der Immersion des virtuellen Raums begründet: Die durch die VR-Technologie vermittelte realistische Wahrnehmung der virtuellen Umgebung sowie die dadurch bedingte „Verkörperung" der eigenen Person im Avatar führen dazu, dass die individuellen Grenzen des körperlichen Nähebewusstseins (Proxemik) in das Metaverse übertragen werden.[18] Unerwünschte Annäherungen fremder Avatare können daher als Verletzung der

16 *Benrimoh u.a.*, The Best Predictor of the Future, JMIR Mental Health 2022, 1 (4).
17 *Franks*, The Desert of the Unreal, UC Davis Law Review 2017, 499.
18 *Mello u.a.,* The influence of body expression, group affiliation and threat proximity on interactions in virtual reality, Current Research in Behavioral Sciences 2022, 100075.

individuellen Persönlichkeitssphäre wahrgenommen werden.[19] Gleichzeitig führt die realistische Wahrnehmung des Erlebten zu realen körperlichen Auswirkungen: Während Betroffene kurzfristig unter sog. Freeze-Zuständen leiden können, können mittel- und langfristig sogar psychosomatische Beschwerden wie etwa Angstzustände drohen.[20]

3.1.2 Social Bots

Social Bots sind (teil-)automatisierte Software-Agenten bzw. Computerprogramme, die unter Vortäuschung einer menschlichen Identität am öffentlichen Diskurs im Internet teilnehmen.[21] Im Metaverse können Social Bots insbesondere in Gestalt von Avataren auftreten. Es kommt für die Vortäuschung einer menschlichen Identität nicht darauf an, welche Erscheinungsform der Social Bot – also beispielsweise ob fotorealistisch oder nicht – hat. Entscheidend ist, ob die gewählte Erscheinungsform in der jeweiligen Umgebung eines Metaverse mit menschengesteuerten Avataren assoziiert wird. Als solche sind sie in der Lage, im virtuellen Raum menschenähnlich von „Angesicht zu Angesicht" mit anderen Nutzern zu interagieren.[22] Dies führt dazu, dass eine Unterscheidung zwischen softwaregesteuerten und menschengesteuerten Avataren oftmals gar nicht oder nur mit Mühe möglich ist.[23]

Dieses Täuschungspotential kann aufgrund der breiten Nutzungsmöglichkeiten des Metaverse eingesetzt werden, um umfassend auf Meinungen sowie Entscheidungsmuster menschlicher Nutzer einzuwirken. Social Bots könnten im Metaversum beispielsweise genutzt werden, um im Rahmen personalisierter Interaktionen gezielt Werbung zu verbreiten oder interessierte Nutzer vom Kauf bestimmter Produkte zu überzeugen.[24] Ebenso könnten Social Bots zur Durchführung großer Desinformationskampagnen

19 *Freeman u.a.*, Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality, Proceedings of the ACM on Human-Computer Interaction 2022, 1 (11).

20 *Wiederhold*, Sexual Harassment in the Metaverse, Cyberpsychology, Behavior, and Social Networking 2022, 479.

21 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (94); Dürr, Social Bots, S. 7 ff.

22 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (94).

23 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (54).

24 *Falchuk/Loeb/Neff*, The Social Metaverse: Battle for Privacy, IEEE Technology and Society Magazine 2018 37(2), 52 (53 ff.).

sowie für politische Propaganda missbraucht werden.[25] Schließlich besteht die Gefahr, dass das Verhalten bestimmter Nutzer mittels Social Bots überwacht wird oder durch gezielte, automatisierte Ansprache unbemerkt persönliche Daten gesammelt werden.[26] Im Metaverse können Social Bots selbst auf zusätzlichen Verhaltensebenen menschliches Verhalten vortäuschen, aber auch auf zusätzliche Verhaltensdaten von Nutzern, beispielsweise die Mimik oder Gestik, zugreifen. Dadurch vergrößert sich das Gefahrenpotenzial.

3.2 Gefahren für den Datenschutz

Ein weiteres Feld privatheitsbezogener Probleme im Metaverse betrifft die Datenschutzherausforderungen. Diese ergeben sich vor allem aus der DSGVO, welche die meisten Regelungen zum Schutz natürlicher Personen vor der Verarbeitung ihrer personenbezogenen Daten enthält. Zentrale Herausforderungen im Metaverse stellen dabei die intensivere Datenerhebung sowie die unzureichenden Datenschutzerklärungen und -einwilligungen dar.

3.2.1 Intensität und Umfang der Datenerfassung

Ohne die Verarbeitung von personenbezogenen Daten sind moderne Internetanwendungen, wie z.B. Social Media, gar nicht denkbar.[27] Metaverse-Systeme könnten jedoch wesentlich intensiver Informationen sammeln als herkömmliche Systeme. *Happa et al.* äußern Bedenken darüber, dass sämtliche Sensordaten von Geräten potenzielle Quellen für bisher unbekannte multidimensionale Datenschutzrisiken darstellen könnten, die schwerwiegender sind als die aus früheren Technologien bekannten.[28]

---

25 *Dwivedi et al.*, Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse, Information Systems Frontiers 2023, 25, 2071 (2083).

26 *Falchuk/Loeb/Neff*, The Social Metaverse: Battle for Privacy, IEEE Technology and Society Magazine 2018, 37(2), 52 (53 ff.).

27 So auch *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (4).

28 *Happa u.a.*, Privacy-certification standards for extended-reality devices and services, IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, Lisbon 2021, 397 (397).

Ein wesentlicher Unterschied zwischen dem Metaverse und dem herkömmlichen Internet besteht dabei in der Echtzeitverfolgung von physiologischen Daten und von Bewegungsdaten.[29] Über Technologien wie z.B. VR-Brillen, Controller, spezielle Anzüge oder Schuhe, welche zur Interaktion zwischen Nutzern und dem Metaverse genutzt werden, können Gesichtsausdrücke, Gangart sowie Augen-, Kopf- und Handbewegungen verfolgt werden. Solche Headsets und andere Geräte könnten vielfältige biometrische Daten sammeln, einschließlich Stimmprofile, Gesichtsgeometrie, Iris- und Netzhautscans, Handabdrücke, Fingerabdrücke sowie Gehirn- und Herzsignale. Neurophysiologische Daten, wie Gehirnwellenmuster und neuronale Aktivitäten, können ebenfalls erfasst werden, entweder durch Sensoren oder Gehirn-Computer-Schnittstellen.

Die im Metaverse genutzten Avatare können zudem das Aussehen der realen Nutzer widerspiegeln.[30] Dies kann Aufschluss geben über ihre ethnische Herkunft und ihr Geschlecht.[31] Die Bewegungen und Gesichtsausdrücke der Nutzer können in den Avataren wiedergegeben werden, um ein realistischeres Erlebnis zu bieten.[32] Verhalten und Vorlieben können durch Interaktionen mit virtuellen Objekten und anderen Avataren[33] sowie durch

29 *Di Pietro/Cresci*, Metaverse: Security and Privacy Issues, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, Atlanta 2021, 281 (284); *Marloth u.a.*, Psychiatric Interventions in Virtual Reality, Cambridge Quarterly of Healthcare Ethics 2020, 574 (579 f.); *Ruiz Mejia/Rawat*, Recent Advances in a Medical Domain Metaverse, International Conference on Ubiquitous and Future Networks, Barcelona 2022, 357 (358).

30 *Awadallah u.a.*, Identity Threats in the Metaverse and Future Research Opportunities, International Conference on Business Analytics for Technology and Security, Dubai 2023, 1 (3); *Venugopal u.a.*, The realm of metaverse, Computer Animation and Virtual Worlds 2023, 1 (8).

31 *Maloney u.a.*, Anonymity vs. Familiarity, ACM Symposium on Virtual Reality Software and Technology 2020, 1 (7); *Vladimirov u.a.*, Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse, International Scientific Conference on Information, Communication and Energy Systems and Technologies, Ohrid 2022, 1 (1 f.); *Wang u.a.*, Shared realities, ACM on Human-Computer Interaction 2021, 1 (4).

32 *Awadallah u.a.*, Identity Threats in the Metaverse and Future Research Opportunities, International Conference on Business Analytics for Technology and Security, Dubai 2023, 1 (2); *Smith u.a.*, The World as an Interface, Hawaii International Conference on System Sciences 2023, 6045 (6048 f.).

33 *Fernandez/Hui*, Life, the Metaverse and Everything, IEEE International Conference on Distributed Computing Systems Workshops, Bologna 2022, 272 (273).

Eye-Tracking und physische Bewegungen[34] offengelegt werden. Emotionen können durch Kameras, drucksensitive Brillen für Gesichtsmuskulaturbewegungen,[35] Spracherkennung[36] oder aus anderen Daten wie Augen- und Körperbewegungen oder Herzfrequenz[37] abgeleitet werden.

Schließlich sehen *Falchuk et al.* noch das Risiko, dass Avatare auf der Metaverse-Plattform keine Möglichkeit haben, sich selbst vor der Datenerfassung zu verbergen.[38] Nutzer könnten sich daher unbeabsichtigt einer im Hintergrund stattfindenden Datenüberwachung aussetzen.[39]

Hinzu kommen Kontextdaten. Die Metaverse-Plattformen können mithilfe von Datenanalysesoftware die Aktivitäten der Avatare überwachen und analysieren, um Einblicke in die Nutzung der Dienste durch die Nutzer zu ermöglichen.[40] So ließen sich virtuelle Laufwege, Besuche virtueller Orte, Reaktionen der Nutzer auf Produkte oder Ereignisse und weitere Daten sammeln.

3.2.2 Immersive Datenschutzerklärungen und Einwilligungen

In aktuellen Metaverse-ähnlichen Systemen werden Nutzer selten umfassend über die Datenerhebung und -verarbeitung aufgeklärt.[41] Datenschutz-

34 *Dwivedi u.a.*, Exploring the Darkverse, Information Systems Frontiers 2023, 2071 (2075); *Smith u.a.*, The World as an Interface, Hawaii International Conference on System Sciences 2023, 6045 (6049); *Tricomi u.a.*, You Can't Hide Behind Your Headset, IEEE Access 2022, 9859 (9864).

35 *McStay*, The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons, Philosophy and Technology 2023, 1 (6).

36 *Smith u.a.*, The World as an Interface, Hawaii International Conference on System Sciences 2023, 6045 (6051 ff.).

37 *Abraham u.a.*, Implications of XR on Privacy, Security and Behaviour, Nordic Human-Computer Interaction Conference, Aarhus 2022, 1 (9); *Happa u.a.*, Privacy-certification standards for extended-reality devices and services, IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, Lisbon 2021, 397 (397).

38 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (55).

39 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (54).

40 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (53 f.); *Awadallah u.a.*, Identity Threats in the Metaverse and Future Research Opportunities, International Conference on Business Analytics for Technology and Security, Dubai 2023, 1 (3).

41 *Abraham u.a.*, Implications of XR on Privacy, Security and Behaviour, Nordic Human-Computer Interaction Conference, Aarhus 2022, 1 (5).

richtlinien sind oft unzureichend, besonders hinsichtlich VR-spezifischer Datensammlung,[42] und viele soziale Metaverse-Plattformen informieren Nutzer nicht ausreichend über ihre Datenschutzeinstellungen, was dazu führt, dass Daten möglicherweise unwissentlich (für Dritte) geteilt werden.[43] Die DS-GVO fordert, dass über Datenverarbeitungen transparent und verständlich kommuniziert wird, Art. 13, 14 DS-GVO; dies wird jedoch selten erfüllt.[44] Datenschutzerklärungen sind oft zu lang, unübersichtlich und in schwer verständlicher juristischer Fachsprache verfasst. Zum Beispiel umfasst die Datenschutzerklärung von Roblox[45] 13.607 Wörter, was etwa 26 DIN A4 Seiten entspricht und fast 62 Minuten Lesedauer erfordert. Erschwerend kommt hinzu, dass bereits der Mitteilungsweg der Datenschutzinformationen in Metaverse-Anwendungen unklar ist; denkbar sind z.B. Einblendungen, virtuelle Aushänge oder Verlinkungen auf Webseiten.[46]

Darüber hinaus müssen im Metaverse viele Datenverarbeitungsprozesse auf eine Einwilligung als Rechtsgrundlage gestützt werden (Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DS-GVO), insbesondere wenn es um die Verarbeitung sensibler personenbezogener Daten wie Gesundheitsdaten (z. B. Herzfrequenz) geht. Nach Art. 4 Nr. 11 DS-GVO muss die Einwilligung in informierter Weise, freiwillig und granular bestimmt für alle Zwecke der Verarbeitung erfolgen.[47] Im Kontext herkömmlicher Websites wird dies häufig durch Cookie-Banner umgesetzt, die den Nutzern die Möglichkeit geben, über die Verwendung ihrer Daten zu entscheiden.

Im Metaverse gestaltet sich die Umsetzung dieser Anforderung jedoch ungleich komplexer. Das immersive Erlebnis, welches das zentrale Merkmal dieser virtuellen Welten ist, steht im Spannungsfeld mit den datenschutz-

42 *Adams u.a.*, Ethics Emerging, USENIX Symposium on Usable Privacy and Security 2018, 443 (451).

43 *Kang u.a.*, Security and Privacy Requirements for the Metaverse, IEEE Communications Magazine 2023, 148 (150 ff.); *Maloney u.a.*, Anonymity vs. Familiarity, ACM Symposium on Virtual Reality Software and Technology 2020, 1 (2 ff.).

44 *Kettner u.a.*, Innovatives Datenschutz-Einwilligungsmanagement, 2020, S. 12.

45 *Roblox*, Roblox-Datenschutz- und Cookie-Richtlinie, 2025.

46 Vgl. *Klar u.a.*, Datenschutz im Metaverse, BB 2022, 2691 (2694); *Benedikt*, in: Steege/Chibanguza, Metaverse, 2023, § 11, Rn. 57.

47 Vgl. zur Diskussion um die fragliche Freiwilligkeit bei Einwilligung im Kontext sozialer Netzwerke *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DS-GVO, Rn. 53 ff. m.w.N.

rechtlichen Vorgaben.[48] Auf zentralisierten Plattformen könnte es zwar möglich sein, datenschutzrechtliche Informationen in Textform im Vorfeld des „Eintauchens" bereitzustellen: Nutzer könnten vor dem Zugang zu einer immersiven Umgebung über die wesentlichen Verarbeitungszwecke aufgeklärt und um ihre Zustimmung gebeten werden.

Problematisch wird diese Vorgehensweise jedoch, wenn ein Blick auf die Vision des Metaverse geworfen wird: Durch seine grenzüberschreitende und dynamische Struktur soll es über die rein technischen und rechtlichen Grenzen eines einzelnen Anbieters hinausgehen. Wenn Nutzer in einen neuen Verantwortungsbereich überwechseln – beispielsweise beim Betreten eines virtuellen Raumes, der von einem anderen Anbieter bereitgestellt wird - -müsste erneut eine datenschutzrechtliche Information erfolgen und gegebenenfalls eine neue Einwilligung eingeholt werden.

Diese Anforderung kollidiert mit dem Prinzip einer nahtlosen, immersiven Erfahrung, da Unterbrechungen zur Information oder Einholung von Einwilligungen das Nutzungserlebnis beeinträchtigen könnten. Die Herausforderung besteht daher darin, ein datenschutzkonformes Informations- und Einwilligungsmanagement zu entwickeln, das einerseits den gesetzlichen Anforderungen entspricht und andererseits die immersiven Eigenschaften des Metaverse nicht beeinträchtigt.

4. Lösungsoptionen durch Privacy-by-Design-Praktiken

Um angesichts der genannten Herausforderungen den Schutz der Privatheit zu gewährleisten, ist es entscheidend, den Privacy-by-Design-Ansatz zu verfolgen. Dieser technische und strategische Managementansatz zielt darauf ab, dass der Schutz der Privatheit bereits zu Beginn proaktiv in die Konzeption und Entwicklung des Metaverses integriert werden muss, anstatt ihn erst im Nachhinein zu berücksichtigen.[49] Dadurch können Risiken präventiv und nachhaltig minimiert werden.

Der Europäische Gesetzgeber und andere Gesetzgeber legen großen Wert auf den Privacy-by-Design-Ansatz, um eine ausgewogene Balance

48 Dwivedi *u.a.,* Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse, Information Systems Frontiers 2023, 2071; Europäische Kommission, Datenschutz und Privatsphäre in virtuellen Welten, 2025.

49 *Spiekermann*, The challenges of privacy by design, Communications of the ACM 2012, 38.

zwischen den Privatheitsbedürfnissen der Nutzer und den Datenanforderungen von Unternehmen und der Regulierung zu erreichen.[50] Dennoch bleibt das Konzept oft abstrakt und schwer umzusetzen, da es an konkreten Anforderungen fehlt, insbesondere im Kontext aufkommender Technologien.[51] Daher wird in diesem Beitrag versucht, konkrete Implementierungen für das Metaverse zu erarbeiten, um ein sicheres und datenschutz- wie persönlichkeitsrechtsfreundliches Metaverse zu schaffen.

Die Entwicklung der Designvorschläge wurde mit einer systematischen Analyse der Forschungs-, Praxis- und Rechtsliteratur eingeleitet, ergänzt durch die Auswertung ausgewählter Metaverse-Plattformen sowie semistrukturierter Experteninterviews. Die Zielsetzung bestand zunächst in der Identifizierung der drängendsten Problemfelder des Metaverse. In einem nachfolgenden Schritt wurden die identifizierten Problemfelder und ersten Designvorschläge in einem partizipativen Format mit Experten diskutiert. Im Rahmen dieser Diskussion wurden die Vorschläge hinsichtlich ihrer Effektivität und Umsetzbarkeit priorisiert.

Die folgende Darstellung beschränkt sich auf einen Ausschnitt der Forschung und soll das Vorhaben und die Ergebnisse exemplarisch an ausgewählten Beispielen illustrieren. Ein besonderer Fokus liegt dabei auf dem persönlichkeitsrechtlichen Problemfeld der virtuellen Belästigung und dem datenschutzrechtlichen Problemfeld der Datenschutzerklärungen und Einwilligungen in immersiven virtuellen Welten. Aber auch weitere Designvorschläge sollen beispielhaft erläutert werden, um die Vielfalt der möglichen Ansätze anzudeuten.

4.1 Virtuelle Belästigung (Persönlichkeitsrechte)

Anders als in der realen Welt existieren im Metaverse (noch) keine spezifischen gesetzlichen Rahmenbedingung, die in der Lage wären, Belästigungen und andere „virtuell-physischen" Schädigungen zu verhindern. Bestehende Vorgaben des Strafrechts, des Persönlichkeitsrechts oder des Datenschutzrechts finden zwar grundsätzlich Anwendung, leiden jedoch unter einem generellen Durchsetzungsproblem und sind nicht zugeschnitten auf die besonderen Situationen und Probleme von Metaversen. Gleichzeitig

50 *Spiekermann*, The challenges of privacy by design, Communications of the ACM 2012, 38.

51 *Bu u.a.*, „Privacy by Design" implementation: Information system engineers' perspective, International Journal of Information Management, 102124, 3.

ist jedoch deutlich geworden, dass virtuelle Übergriffe mitunter ebenso einschneidend wahrgenommen werden können, wie vergleichbare Ereignisse in der „echten" Welt. Dies führt dazu, dass Plattformbetreiber mehr denn je in der Verantwortung stehen, virtuelle Belästigungen durch privatheitsfreundliche Designstrategien proaktiv zu verhindern oder jedenfalls zu erschweren. Dabei sollten Plattformdesigns im Vordergrund stehen, die einerseits Anreize für mögliche Belästigungssituationen reduzieren und andererseits Nutzern die jederzeitige Kontrolle über ihre Interaktionen ermöglichen. Daneben können Plattformbetreiber die Verantwortlichen auch sanktionieren. Maßnahmen könnten neben kurzfristigen Nutzungsverboten auch eine Sperrung des Kontos sein. Entsprechende Regelungen könnten Einzug in die Allgemeinen Geschäftsbedingungen der Nutzungsverträge finden.

Zur Prävention virtueller Belästigungen im Metaverse erscheinen insbesondere jene Designvorschläge geeignet, die durch eine privatheitsfreundliche Gestaltung des virtuellen Raums die Auswirkungen derartige Übergriffe so gering wie möglich halten. Eine potenzielle Designpraktik stellt etwa die Einrichtung einer virtuellen Sicherheitszone dar, in welcher Nutzer vor der Annäherung anderer Avatare geschützt sind. Bei dem „Scheinwerfer"-Design wird den angegriffenen Nutzern die Möglichkeit verschafft, besondere Aufmerksamkeit auf den Aggressor zu richten, sodass dieser von seinem Opfer ablässt. Darüber hinaus kann auch das generelle Design eines virtuellen Raums zur Prävention virtueller Belästigungen beitragen.

4.1.1 Helle Beleuchtung und soziale Kulisse durch Bots

Um virtuelle Belästigungen proaktiv vorzubeugen, wurde bei der Gestaltung öffentlicher virtueller Räume gezielt mit sogenannten Nudges gearbeitet, um situative Faktoren zu beeinflussen, die Belästigungen begünstigen können. Ein zentraler Auslöser für antinormatives und deviantes Verhalten ist der Enthemmungseffekt, der unter anderem durch die Unsichtbarkeit und dissoziative Anonymität entsteht.[52]

Dunkle, schwach beleuchtete Bereiche können das Gefühl der Anonymität und Verantwortungslosigkeit verstärken, da sich die Täter weniger sicht-

52 *Hirsch, u.a.,* Drunk, Powerful, and in the Dark: How General Processes of Disinhibition Produce Both Prosocial and Antisocial Behavior, Perspectives on Psychological Science 2011, 415.; *Suler*, The Online Disinhibition Effect, CyberPsychology & Behavior 2004.

bar und dadurch weniger identifizierbar fühlen.[53] Dies kann prosoziales Verhalten hemmen und unethisches Verhalten begünstigen.[54] Zudem zeigen Studien, dass helle Beleuchtung in öffentlichen Bereichen (z.B. Straßen oder Geschäften) Straftaten reduzieren kann.[55] Dieser Effekt könnte gezielt auf die Gestaltung virtueller Umgebungen übertragen werden, da Nutzer dazu neigen, vertraute Muster aus der physischen Welt auch im virtuellen Raum anzuwenden.

Zudem neigen Täter dazu, Opfer eher in isolierten Situationen zu belästigen, wo keine Dritten anwesend sind, die eingreifen könnten.[56] Solche Täter-Opfer-Szenarien können auch im Metaverse auftreten. Daher könnte eine gezielte Integration zusätzlicher, nicht von Nutzern gesteuerter Avatare diesem Risiko entgegenwirken, indem eine öffentlich wirkende Umgebung simuliert wird. Dadurch entsteht für potenzielle Täter der Eindruck, unter Beobachtung zu stehen, was die Hemmschwelle für Belästigungen erhöht und die Einhaltung respektvoller sozialer Normen stärkt.

4.1.2 Safe Zones

Ein weiterer Ansatz zum Schutz der Nutzer besteht im Erhalt ihres persönlichen Raums, da Belästigungen in virtuellen Welten häufig durch das unbefugte Eindringen in die physische Nähe eines Avatars entstehen.[57] Hier könnten sogenannte Safe Zones helfen – Schutzbereiche, die als Radius um den Avatar eines Nutzers eingerichtet werden und bei Betreten durch andere Avatare bestimmte Reaktionen auslösen. Solche Maßnahmen können auf unterschiedliche Weise umgesetzt werden, um unerwünschte Interaktionen zu minimieren und zu verhindern, dass fremde Avatare zu nahe kommen.

---

53 *Zhong u.a.*, Good Lamps Are the Best Police: Darkness Increases Dishonesy and Self-Interested Behavior, Psychological Science 2010.

54 *Liu u.a.*, Gender moderates the effect of darkness on ethical behaviors: An explanation of disinhibition, Personality and Individual Differences 2018.

55 *Fotios u.a.*, The Effect of Lighting on Crime Counts, Energies 2021, 4099; *Chalfin u.a.*, Reducing Crime Through Environmental Design, Journal of Quantitative Criminology 2022, 127; *Mitre-Becerril u.a.*, Can deterrence persist?, Criminology & Public Policy 2022, 865.

56 *Painter*, The influence of street lightning improvements on crime, fear and pedestrian street use, after dark. Landscape and Urban Planning 1996.

57 *Freeman u.a.*, Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality, Proceedings of the ACM on Human-Computer Interaction 2022.

Präventiv eingesetzt, bildet eine Safe Zone einen unsichtbaren Schutzkreis um den Avatar des Nutzers, sodass andere Avatare den dadurch bestimmten Abstand zum Avatar des Nutzers einhalten müssen, um gesehen und gehört zu werden. Bei Überschreiten dieser Grenze werden sie automatisch unsichtbar und stummgeschaltet. Die Sicherheitszone ist für andere Avatare individuell einstellbar, d.h. Nutzer können bestimmten Avataren (z.B. Freunden) erlauben, den Kreis zu betreten, ohne dass diese ausgeblendet werden.

Reaktiv eingesetzt, kann eine Safe Zone im Falle eines Übergriffs aktiviert werden. Der Schutzkreis dient in dieser Version dazu, den Sicherheitsabstand zu anderen Avataren zu erzwingen. Avatare, die sich innerhalb dieses Schutzkreises aufhalten, werden ebenfalls unsichtbar und unhörbar gemacht. Gleichzeitig wird der Avatar des Nutzers auch für andere Avatare ausgeblendet, sobald sie ihm zu nahe kommen.

In manchen Fällen reicht eine Safe Zone allein nicht aus, da Belästigungen auch aus der Distanz durch zulässige Interaktionsmöglichkeiten erfolgen können. Deshalb ist es sinnvoll, diesen Schutzmechanismus mit weiteren Funktionen, wie z.B. einer Blockfunktion zu kombinieren. Dadurch können Avatare der Täter und ihre Handlungen unabhängig von der Entfernung für betroffene Nutzer unsichtbar und unhörbar gemacht werden. Gleichzeitig werden auch der Avatar und die Aktivitäten des Opfers in der virtuellen Umgebung für die Täter nicht mehr sichtbar oder hörbar.

4.2 Kennzeichnung von Social Bots und Bot-freie Zonen (Persönlichkeitsrechte)

Im Hinblick auf Social Bots kann den Gefahren einer Identitätstäuschung insbesondere mittels einer identifizierenden Kennzeichnung KI-gesteuerter Avatare oder durch vorgelagerte Identitätskontrollen begegnet werden. Die visuelle Kennzeichnung von Bots könnte beispielsweise durch Beschriftungen, Symbole, Umrandungen oder durch die Verwendung bot-spezifischer Avatare umgesetzt werden, um Nutzern die Interaktion mit einer KI offenzulegen. Eine solche visuelle Kennzeichnung ist für „Verwender" von Social Bots auch verpflichtend nach § 18 Abs. 3 Medienstaatsvertrag.[58] Nach der KI-Verordnung gilt eine vergleichbare Kennzeichnungspflicht mittlerweile

58 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (95).

auch für Entwickler, Art. 50 KI-Verordnung.[59] Betreiber von Metaversen werden nicht durch § 18 Medienstaatsvertrag oder Art. 50 KI-Verordnung in die Pflicht genommen. Entwickler und auch Verwender von Social Bots sind jedoch oftmals von den technischen Gegebenheiten und Vorgaben von Plattformbetreibern abhängig. Deshalb besteht eine Effektuierungspflicht für Plattformbetreiber nach § 93 Medienstaatsvertrag. Demnach sollen zumutbare Anstrengungen zur Sicherstellung einer Kennzeichnung vorgenommen werden.[60] Vorgelagerte, privatheitsfreundliche Identitätskontrollen könnten mithilfe der flächendeckenden Einführung von 3D-Captchas ermöglicht werden: Avatare, die als Bots verdächtigt werden, müssten demnach kleine Aufgaben in der 3D-Umgebung lösen, um ihre menschliche Identität zu bestätigen.

Um einige der genannten Gefahren zu verhindern, z.B. potenzielle Bot-gestützte Desinformationskampagnen, kann es notwendig sein, über eine reine Kennzeichnungspflicht hinauszugehen. Neben einem kompletten Verbot von Social Bots in Metaversen können bot-freie Zonen als weniger intensive Maßnahme konstituiert werden. Bot-freie Zonen sind Bereiche, in denen die Verwendung von KI-gesteuerten Avataren generell unterbunden wird, sodass Nutzer dort nur auf menschengesteuerte Avatare treffen können.

4.3 Sensorhinweise (Datenschutz)

Zur Reaktion auf die gesteigerte Intensität und den gesteigerten Umfang der Datenerfassung könnten u.a. dauerhafte Sensorhinweise, punktuelle Aktivierungsabfragen sowie eine standardmäßige Zeitbegrenzung der Sensortätigkeiten dienen. Ersteres wäre durch farbliche Hinweise im Sichtfeld des Nutzers umsetzbar, die z.B. auf das Tracking von Pulsmessern oder Eye-Tracking hinweisen. Die punktuelle Aktivierungsabfrage fordert, abhängig von der jeweiligen Anwendungssituation, gezielt die Zustimmung des Nutzers zur Aktivierung bestimmter Sensoren an, und schafft dadurch ein erhöhtes Bewusstsein für die Datenerfassung in sensiblen Situationen. Berechtigungsabfragen haben sich in mobilen Anwendungskontexten bereits als wirksames Mittel erwiesen, um das Risikobewusstsein der Nutzer in Bezug auf ihre Privatheit zu stärken. Kombiniert mit einer regelmäßig

59 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (98).
60 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (97).

zu erneuernden Freigabe der jeweiligen Datenströme, die den Nutzer daran erinnert, welche Sensoren aktiv sind und erneut um Freigabe der Datenströme bittet, wird die Datensouveränität der Nutzer gestärkt.

4.4 Datenschutzcockpits und Einwilligungsassistenten (Datenschutz)

Um Datenverarbeitungen in immersiven Umgebungen erfolgreich für Nutzer zu kommunizieren (immersive Datenschutzerklärungen), könnten Datenschutzcockpits eingesetzt werden.[61] Die Idee von Datenschutzcockpits wurde bereits im Kontext von Websites angedacht. Diese stellen Informationen zu Datenverarbeitungen sowie Verarbeitungszwecken nutzerfreundlich und in einer Übersicht mit Einstellungsmöglichkeiten dar, was sowohl plattformspezifisch als auch anwendungsspezifisch ausgestaltet sein kann.[62] Eine weitere Lösungsidee könnten unterstützende Gestaltungselemente als Teil der Datenschutzerklärung sein. Dies umfasst Datenschutzicons und Strukturierung durch Abschnittsstrukturen – ggf. auch videogestützt.

Eine immersivere und somit weitergehende Lösung für die datenschutzrechtlichen Herausforderungen im Metaverse könnte ein virtueller Informations- und Einwilligungsassistent („Stefan Schild“[63]) darstellen, der eine dynamische und nutzerfreundliche Verwaltung von datenschutzrechtlichen Informations- und Einwilligungsprozessen ermöglicht. Dieser Assistent sollte sich nahtlos in die immersive Umgebung integrieren und als ständiger Begleiter der Nutzer fungieren, um auf Wunsch relevante Datenschutzinformationen bereitzustellen und Einwilligungen einzuholen, ohne das immersive Erlebnis im Metaverse zu unterbrechen.

Stefan Schild könnte personalisiert und kontextsensitiv agieren. Sobald ein Nutzer in einen neuen Verantwortungsbereich eintritt, z.B. beim Wechsel von einer Plattform zu einer anderen oder beim Besuch eines virtuellen Raums, der von einem Drittanbieter verwaltet wird, würde der Assistent die jeweiligen datenschutzrechtlichen Anforderungen im Hintergrund analysieren. Er würde in Echtzeit eine benutzerfreundliche, kontextabhängige Benachrichtigung ausspielen, welche die wichtigsten Informationen zur

61 *Gerpott*, Datenschutzerklärungen – Materiell fundierte Einwilligungen nach der DS-GVO, MMR 2020, 739 (742).

62 Vgl. *Kettner u.a.*, Wege zur besseren Informiertheit, 2018, S. 71 ff., die das Konzept „Privacy Bots“ nennen. Ebenso *Nüske u.a.*, Privacy Bots, DuD 2019, 28.

63 Bei „Stefan Schild“ handelt es sich um einen willkürlichen Arbeitstitel, der lediglich einen illustrierenden Mehrwert hat.

Datenverarbeitung kurz und prägnant zusammenfasst. Zudem könnte der Assistent die erforderliche Einwilligung einholen.

Anstelle aufdringlicher Pop-ups könnte Stefan Schild in Form eines diskreten, interaktiven Avatars oder einer symbolischen Benutzeroberfläche auftreten, die jederzeit ansprechbar ist. So könnten Nutzer durch einfache Sprachbefehle, Gesten oder Klicks mehr Details zu den Datenschutzinformationen abrufen oder ihre Einwilligung für spezifische Verarbeitungen erteilen oder verweigern. Dadurch könnte Stefan Schild zudem fortlaufend Transparenz gewährleisten, indem er Nutzer aktiv darüber informiert, welche Daten wann und zu welchem Zweck verarbeitet werden. Um das Erlebnis mit Stefan Schild motivierender zu gestalten, könnten Gamifizierungselemente wie Belohnungssysteme, Personalisierung und eine spannende Hintergrundgeschichte integriert werden. Der Assistent könnte wiederum mit anderen Ansätzen kombiniert werden, wie etwa Icons oder Videos.

5. Testung der Designs in Fokusgruppen

Die beschriebenen Designoptionen können nur dann zum Schutz der Privatheit im Metaverse beitragen, wenn sie von den Nutzern des Metaverse als unterstützend und sinnvoll wahrgenommen werden. Die Reaktionen potenzieller Nutzer auf die Designoptionen wurden daher in einem qualitativen und explorativen Format in Fokusgruppen getestet. Durch ein Marktforschungsinstitut wurden insgesamt vier Gruppen zusammengestellt. Davon waren zwei Gruppen mit „metaverse-affinen" Nutzern besetzt, die selbst im Besitz einer VR-Brille waren, die in den zwei anderen Gruppen vertretenen Nutzer besaßen keine VR-Brille. Ansonsten waren alle Gruppen divers zusammengesetzt mit Blick auf Geschlecht, Altersverteilung, Bildungsstand und Wohnort (ländlich/städtisch). Drei Gruppen hatten jeweils sieben Teilnehmer, die Gruppe der metaverse-affinen Nutzer im Bereich der Persönlichkeitsrechte hatte sechs Teilnehmer.

In jeweils zwei Fokusgruppen wurden vertieft die Designoptionen zum Schutz der Persönlichkeitsrechte sowie die Designoptionen aus dem Bereich des Datenschutzes getestet. Dabei wurde zu jedem Teilaspekt des Vorhabens einmal die Perspektive metaverse-affiner Nutzer untersucht und einmal die Perspektive sonstiger Nutzer.

5.1 Quantitative Auswertung der Fokusgruppen

In den Rückmeldungen aus den Fokusgruppen wurden deutliche Unterschiede zwischen der Wahrnehmung der Designs in den Bereichen Persönlichkeitsrechte und Datenschutz erkennbar, wie nachstehend im Einzelnen beschrieben wird. Eine Übersicht zur Wahrnehmung der Designoptionen ist in der Abbildung enthalten. Als quantitative Wertung haben die von den Probanden der Fokusgruppen getroffenen Einschätzungen aufgrund der geringen Anzahl der Teilnehmer nur eine begrenzte Aussagekraft. Sie werden daher im Folgenden vor allem zu dem Zweck genannt, um die nachstehend erläuterten qualitativen Einschätzungen der Probanden zu illustrieren (vgl. Tabelle 1).

5.2 Qualitative Auswertung der Fokusgruppen

Mehr noch als die quantitativen Ergebnisse ist die qualitative Auswertung der Fokusgruppen für die Implementierung eines Privacy-by-Design-Ansatzes im Metaverse relevant. In den Fokusgruppen wurde zunächst jeweils die allgemeine Haltung der Teilnehmer zu Fragen der Privatheit im Metaverse diskutiert, sodann die Wahrnehmung unterschiedlicher Designoptionen zum Schutz der Privatheit. Die qualitative Auswertung der Fokusgruppen wird nachstehend gegliedert nach den Aspekten der Persönlichkeitsrechte und des Datenschutzes wiedergegeben.

5.2.1 Persönlichkeitsrechte

5.2.1.1 Risikowahrnehmung

In allen Fokusgruppen wurden die Risiken des Metaverse im Bereich der Persönlichkeitsrechte als relevant angesehen; für etliche Probanden auch als Grund genannt, das Metaverse selbst nicht nutzen zu wollen (*„wenn ich jetzt da regelmäßig belästigt würde im Metaverse, wieso benutzt man es dann überhaupt noch?“*). Es wurde allgemein als wahrscheinlich angesehen, dass die aus der digitalen Welt bereits bekannten Persönlichkeitsrechtsverletzungen im Metaverse eine neue Intensitätsstufe erreichen würden. Dabei fiel auf, dass die weiblichen Teilnehmer der Fokusgruppen eine deutlich höhere Sensibilität gegenüber den Bedrohungen ihrer Persönlichkeitsrechte zeigten als die männlichen Teilnehmer. Unterschiedlich wurde auch einge-

schätzt, inwieweit die Technik imstande sein wird, die Risiken im Bereich der Persönlichkeitsrechte zu minimieren. Auf Seiten einiger männlicher Probanden war ein ausgeprägter Technikoptimismus festzustellen, während von einigen der weiblichen Probanden eher auf die Zusammenhänge zu generellen Fragen im Verhältnis der Geschlechter verwiesen wurde.

Tabelle 1: Übersicht zur Wahrnehmung der Designoptionen

Design	**Gruppe**	**Positiv**[64]	**Neutral**	**Negativ**
Helle Beleuchtung	Affin	0	3	4
	Nicht-affin	1	1	4
	Gesamt	1	4	8
Safe Zones	Affin	4	3	0
	Nicht-affin	0	6	0
	Gesamt	4	9	0
Botkennzeichnung	Affin	6	1	0
	Nicht-affin	4	2	0
	Gesamt	10	3	0
Bot-freie Zonen	Affin	3	4	0
	Nicht-affin	5	1	0
	Gesamt	8	5	0
Sensorhinweise	Affin	1	5	1
	Nicht-affin	5	1	1
	Gesamt	6	6	2
Zeitliche Begrenzung der Sensortätigkeit	Affin	2	3	2
	Nicht-affin	7	0	0
	Gesamt	9	3	2
Datenschutzcockpit	Affin	0	7	0
	Nicht-affin	5	2	0
	Gesamt	5	9	0
Einwilligungsassistent	Affin	0	7	0
	Nicht-affin	3	1	3
	Gesamt	3	8	3

64 Die Probanden wurden jeweils gefragt: Halten Sie die vorgestellten Designoptionen für wirksam? Die Zahl der Probanden, welche die Designoption für wirksam hielten, wird jeweils mit „Positiv" angegeben, die Zahl der Probanden, welche die Designoption für unwirksam hielten, mit „Negativ", die Zahl der Probanden, welche unentschieden waren, wird mit „Neutral" angegeben.

5.2.1.1 Wahrnehmung der Designoptionen

Entsprechend dieser generellen Haltung wurde die Zielsetzung der Designs zum Schutz der Persönlichkeitsrechte allgemein befürwortet und gutgeheißen. Mit Blick auf ihre Wirksamkeit wurden die verschiedenen Designoptionen jedoch unterschiedlich eingeschätzt; außerdem eröffneten die Rückmeldungen aus den Fokusgruppen wichtige Perspektiven zu unbeabsichtigten Nebenwirkungen und zu alternativen Ausgestaltungsmöglichkeiten.

Das Problem der Social Bots war den Probanden aus sozialen Netzwerken bekannt. Daher war auch die Sorge verbreitet, dass sich dieses im Metaverse noch verstärken könnte. Zudem wurde auch das Risiko des Identitätsdiebstahls diskutiert, etwa dass im Metaverse eine reale Person optisch nachgebaut werden könnte. Die Kennzeichnungspflicht für Bots wurde dementsprechend allgemein für gut befunden. In der Ausgestaltung wurden solche Varianten befürwortet, die Bots intuitiv und deutlich von Menschen unterschieden. Die Umsetzbarkeit der Bot-Kennzeichnung wurde allerdings von einigen angezweifelt, da es den Metaverse-Unternehmen an wirksamen Anreizen fehlen würde, für eine Transparenz der Bots zu sorgen. Viel Zuspruch bekam auch die Idee, bot-freie Zonen einzurichten.

Wenig Unterstützung fand demgegenüber der Vorschlag, Metaverse-Umgebungen generell hell auszuleuchten und dadurch potentielle Übergriffe zu erschweren. Zum einen wurde schon die Wirksamkeit dieser Maßnahme in Zweifel gezogen (*„wenn man sich jetzt unsere echte Welt anschaut, passiert sowas schon im Schwimmbad am helllichten Tag“*). Zum anderen wurde kritisiert, dass schummrige Orte eben auch zum Nutzererlebnis des Metaverse gehören würden und dass die gesuchte Atmosphäre durch die helle Ausleuchtung zerstört würde.

Die Idee einer Safe Zone, die vor Übergriffen schützt, fand allgemein Unterstützung. Hier gab es allerdings zur Ausgestaltung einige beachtenswerte Hinweise: Ein punktuelles Scheinwerferlicht auf eine Gefährdungssituation wurde als unwirksam bezeichnet, da die hierdurch erzeugte Aufmerksamkeit möglicherweise genau das sei, was die übergriffige Person suche. Eine „Bubble“, in der eine angegriffene Person für den Angreifer unsichtbar wird, wurde als unfair kritisiert, da sie eher das Opfer als den Gefährder belasten würde; eigentlich sollte der Gefährder ausgeblendet werden. Eine Teilnehmerin schlug vor, dass anstelle der Aktivierung einer Safe Zone im Falle eines Übergriffs von vornherein Mindestabstandszonen programmiert sein sollten, die nur mit expliziter Einwilligung reduziert oder geöffnet werden könnten. Schließlich wurde wiederholt die Idee einer

Moderation des sozialen Geschehens im Metaverse vorgeschlagen, um auch im Vorfeld von technischen Barrieren eine einladende und kommunikationsfördernde Atmosphäre im Metaverse zu schaffen.

5.2.2 Datenschutz

5.2.2.1 Risikowahrnehmung

Im Bereich des Datenschutzes war das Risiko- und Problembewusstsein weniger eindeutig als im Bereich der Persönlichkeitsrechte. Das Thema Datenschutz wurde von einem Probanden als „*sehr aufgebläht*" bezeichnet, und allgemein war eine Resignation gegenüber den datenschutzinvasiven Geschäftsmodellen der heutigen digitalen Welt erkennbar („*die Datensammelei und die Analyse können wir eh nicht komplett abschaffen*").

Interessant waren vor diesem Hintergrund die Einschätzungen der Probanden zu ihrem persönlichen Umgang mit den Datenschutzrisiken im Metaverse. Insbesondere die eher digital- und metaverseaffinen Probanden fanden die invasive Datenerhebung zwar ärgerlich, sahen darin letztlich aber keinen Grund, das Metaverse nicht zu nutzen („*Man hat ja ein Ziel (…) und dann kommen da diese Cookie-Meldungen, und dann klickt man die halt weg, (…) und ich denk mal hier wird es dann genauso sein*"). Es gab aber auch andere Haltungen, die in der Quantität und Granularität der im Metaverse erfassten Daten eine neue Risikoqualität sahen („*Das ist, als wäre ich an einen Lügendetektor angeschlossen*").

Bemerkenswert ist auch, dass es keine Bereitschaft der Probanden gab, das Metaverse über Bezahlmodelle zu nutzen, bei denen keine personenbezogenen Daten ökonomisch verwertet würden. Ein wichtiger Beweggrund hierfür war die Sorge, dass der Datenschutz ansonsten kommerzialisiert würde und es zu einer „*Zwei-Klassen-Gesellschaft*" kommen würde.

Dagegen stieß die Forderung, die kommerzielle Nutzung von personenbezogenen Daten durch eine gesetzliche Regelung generell zu verbieten, auf ganz überwiegende Zustimmung – auch im Bewusstsein dessen, dass in der Folge Metaverse-Umgebungen nur in Bezahlformaten nutzbar wären. Trotz der verbreiteten Resignation gegenüber den allgegenwärtigen Praktiken der Datensammlung war ein hohes Problembewusstsein gegenüber den gesellschaftlichen Folgen der trackingbasierten Geschäftsmodelle feststellbar („*Wie viele süchtige Kinder wollen wir uns denn noch heranzüchten?*"). Die Notwendigkeit einer politischen Lösung wurde gerade angesichts der neuen Gefährdungsqualität im Metaverse betont („*Das ist nochmal so ein*

richtig tiefer Schritt in Richtung gläserner Kunde(…) und deshalb muss man politisch eine Reglung treffen").

5.2.2.2 Wahrnehmung der Designoptionen

Die Rückmeldungen zu den Designvorschlägen im Bereich des Datenschutzes waren unterschiedlich danach, ob die Designs nur zusätzliche Informationen vermittelten oder ob sie die eigentlich gewünschte Nutzung störten. Insbesondere die aktiven Nutzer machten in der Diskussion sehr deutlich, dass Datenschutz die Interaktion und das Erlebnis im Metaverse nicht stören solle.

Vor diesem Hintergrund wurden Sensorhinweise, die deutlich machen, welche Daten auf welchen Wegen gerade erhoben werden, allgemein befürwortet – solange sie nicht mit dem eigentlichen Nutzungserlebnis in Konkurrenz stehen. Allerdings wurde von einigen Nutzern gefordert, dass gleichzeitig mit dem Hinweis auf die Datenerhebung auch der Zweck der Datenverarbeitung deutlich gemacht werden solle.

Auch das Datenschutzcockpit, das Datenverarbeitungen und Datenverarbeitungszwecke transparent macht, stieß auf Zustimmung. In der quantitativen Abfrage wurde auch eine automatische zeitliche Begrenzung der Sensoraktivität eher befürwortet (z.B. das Ausschalten der Kamera nach einer Stunde Nutzung mit der Möglichkeit, die Kamera manuell wieder einzuschalten). Allerdings gibt die geäußerte Abneigung gegen Unterbrechungen Anlass zu Zweifeln, ob ein solches Modell praktisch auf Akzeptanz stoßen würde.

Die immersive Umsetzung von Datenschutzerklärungen und Einwilligungen über den digitalen Assistenten Stefan Schild stieß bei den meisten Probanden auf Widerstand. Viele empfanden den digitalen Assistenten als störend und zeitraubend und zeigten keine Bereitschaft, sich damit auseinanderzusetzen („*Wenn ich muss, würde ich nicht darauf achten oder aufs Klo gehen*"). Datenschutzhinweise sollten nach Meinung der meisten Probanden optional angezeigt werden, sodass man sie bei Interesse nachlesen könne, aber nicht gezwungen sei, sich damit auseinanderzusetzen („*eher ein Datenschutzstand oder eine Säule im Shop, wo ich freiwillig hingehen kann*"). Ohne dass hiernach gefragt wurde, kam von einigen Probanden der Vorschlag, dass die datenschutzrechtliche Einwilligung beim Betreten einer Metaverse-Plattform einmalig vorab geklärt werden sollte und dann während der Nutzung der Plattform keine weiteren Einwilligungen mehr

abgefragt werden sollten (Es sei ein „*Abturner*", wenn man bei jedem Eintritt in einen Shop neu entscheiden müsse – „*gut wäre, wenn es einmalig ist und dann nicht nochmal*", wenn man sich im Anschluss an eine Vorabeinwilligung nur noch mit Datenschutzfragen befassen müsste, wenn man die ursprüngliche Entscheidung revidieren wolle).

6. Braucht das Metaverse Personal Information Management Systems (PIMS)?

Wie sich aus der bisherigen Darstellung abzeichnet, sind nicht alle rechtlichen Probleme allein durch Designs lösbar. Besonders anspruchsvoll gestalten sich Designvorschläge zu datenschutzrechtlichen Informationen und Einwilligungen. Das Phänomen der sinkenden Bereitschaft, sich mit datenschutzrechtlichen Fragestellungen zu beschäftigen, ist auch aus „herkömmlichen" datenschutzrechtlichen Informations- und Einwilligungssituationen bekannt und wird dort treffend als sog. „Abnutzungserscheinungen"[65] bei den Betroffenen beschrieben. Wo zunächst eine grundsätzliche Bereitschaft besteht, sich mit dem Schutz der eigenen personenbezogenen Daten zu beschäftigten, lässt diese nach, sobald der Nutzer zu häufig informiert bzw. nach seiner Einwilligung gefragt wird. Hier bedarf es Lösungen, welche die Interessen der Nutzer berücksichtigen, aber zudem mit dem geltenden Recht vereinbar sind. Wie in den Fokusgruppen angedeutet, könnte eine solche Lösung in zentralisierten, vorweggenommenen Mechanismen liegen, die den Nutzerkomfort erhöhen und das Interesse aufrechterhalten. Ob diese wiederum (in allen Fällen) mit dem Datenschutzrecht vereinbar sind, steht auf einem anderen Blatt.

6.1 Vorteile und Reichweite einer zentralen Datenschutzerklärung und Einwilligung

Eine zentrale Datenschutzerklärung ist ein Dokument oder eine digitale Information, die Nutzern umfassend und transparent erklärt, wie und zu welchen Zwecken ihre personenbezogenen Daten verarbeitet werden. Sie enthält gem. Art. 13, 14 DS-GVO Angaben über die Verantwortlichen der

65 *Spindler/Förster*, Privacy-compliant design of Cookie Banners according to the GDPR, JIPITEC 2023, 2 (31).

Datenverarbeitung, die betroffenen Datenkategorien, die Rechtsgrundlagen der Verarbeitung sowie die Rechte der betroffenen Personen. Im Kontext des Metaverse würde eine zentrale Datenschutzerklärung alle relevanten Datenverarbeitungsprozesse auf einer Plattform oder einem Ökosystem abdecken und idealerweise plattformübergreifend gelten, um eine einheitliche und konsistente Informationsbasis für Nutzer zu schaffen.

Eine zentrale Einwilligung bezeichnet die datenschutzrechtliche Zustimmung einer betroffenen Person zu mehreren, u.U. gleichartigen Datenverarbeitungen, die in einem zusammenhängenden, digitalen oder realen Ökosystem stattfinden. Sie ermöglicht es Nutzern, einmalig ihre Einwilligung zu einer Vielzahl von Verarbeitungszwecken zu erteilen, anstatt wiederholt separate Einwilligungen geben zu müssen.

Eine zentrale und vor allem vor das „Eintauchen" in die Metaverse-Welt vorweggenommene Durchführung des datenschutzrechtlichen Informations- und Einwilligungsprozesses böte den Vorteil, dass Nutzer möglichst einmalig ihre Belange des Datenschutzes regeln können und im weiteren Verlauf des Erlebnisses nicht mehr damit behelligt werden.

Die Reichweite einer zentralen Datenschutzerklärung und Einwilligung stellt im Metaverse-Kontext jedoch eine besondere Herausforderung dar. Aufgrund der dynamischen Natur dieser virtuellen, bestenfalls polypolistischen Welt wird es nicht immer möglich sein, im Vorfeld eine Einwilligung für alle Datenverarbeitungsprozesse einzuholen bzw. im Vorhinein umfassend zu informieren. Insbesondere bei plattformübergreifenden Interaktionen oder beim spontanen Wechsel zwischen unterschiedlichen Verantwortungsbereichen wird die traditionelle Einwilligungspraxis an ihre Grenzen stoßen.

Denn wechselt der Verantwortliche für die konkrete Datenverarbeitung, muss neu informiert und neu eingewilligt werden. Dies gilt spätestens ab dem Punkt, wo die Vision des Metaverse als eine virtuelle Realität, in der Verantwortlichkeitsbereiche verschwimmen, erreicht ist. Wenn stetig und in Echtzeit neue Anbieter von Diensten und Interaktionen auf den Metaverseplattformen auftauchen, kann eine solche Entwicklung unmöglich in einer zentralen Datenschutzerklärung und Einwilligung dargestellt werden.

6.2 Lösung durch Einsatz von Personal Information Management Systems (PIMS)?

Eine mögliche Lösung für die besonderen Anforderungen an zentrale Informations- und Einwilligungsmechanismen im dynamischen Kontext des Metaverse könnte im Einsatz von Personal Information Management Systems (PIMS) liegen.[66] Diese technischen Systeme ermöglichen eine zentralisierte Verwaltung von Einwilligungen durch voreingestellte, automatisierte Entscheidungen basierend auf individuellen Präferenzen der Nutzer.[67] Der Vorteil dieser Systeme liegt auf der Hand: Sie reduzieren die Notwendigkeit ständiger Einwilligungen, minimieren sogenannte „Abnutzungserscheinungen" bei den Nutzern und gewährleisten eine konsistentere Datenschutzkontrolle.[68]

Der wesentliche Vorteil gegenüber einer zentralen Einwilligung durch den Nutzer selbst liegt darin, dass die PIMS nach der entsprechenden Einrichtung durch den Nutzer die Einwilligung für diesen übernehmen. Tritt ein neuer Verarbeitungskontext auf, willigen die PIMS nach den Präferenzen des Nutzers für diesen in die Verarbeitung ein. Der Nutzer selbst wird erst mit dem Verarbeitungskontext konfrontiert, wenn dieser nicht mit seinen Voreinstellungen in Einklang zu bringen ist. Allerdings sind die rechtlichen Fragen rund um die Zulässigkeit und die konkrete Ausgestaltung von PIMS bisher nicht abschließend geklärt.

6.2.1 Zulässigkeit einer Einwilligungsstellvertretung durch PIMS

Ein zentraler rechtlicher Streitpunkt ist die Frage, ob PIMS(-Betreiber) als Einwilligungsstellvertreter agieren dürfen.[69] Wird dies bejaht, könnten Nutzer dem PIMS-Betreiber eine Art „Einwilligungs-Vollmacht" erteilen

66 So a. *Bender-Paukens/Werry*, Datenschutz im Metaverse, ZD 2023, 127 (130).

67 Vgl. *Hunter u.a.*, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, 603 (603); *Botta*, Delegierte Selbstbestimmung?, MMR 2021, 946 (946 f.).

68 Vgl. *Schuchardt*, Die (ferne) Zukunft der Cookie-Einwilligung: PIMS und der Weg zu datenschutzfreundlichen Lösungen, DSB 2025, 103 (103); *Kühling/Sauerborn*, PIMS vs. Einwilligung vs. Browsereinstellungen, ZD 2022, 596 (596): „Cookie-Click-Fatigue".

69 Vgl. zu rechtlichen Herausforderungen *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DS-GVO, Rn. 33 ff.; *Jandt*, in: Jandt/Steidle, Datenschutz im Internet, 2025, Kap. IV, Rn. 122 ff.; *Hunter u.a.*, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, 603 (605).

und damit den Prozess der Einwilligung auslagern. Nach Art. 8 Abs. 1 S. 2 DS-GVO können bei Minderjährigen die Sorgeberechtigten an ihrer Stelle die Einwilligung erteilen, was für die grundsätzliche Zulässigkeit einer Einwilligungsvertretung spricht. Die Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB) stützt ebenfalls die Möglichkeit, in bestimmten Fällen Einwilligungen in Stellvertretung rechtlich wirksam abzugeben.[70] Dennoch fehlt bisher eine explizite Regelung in der DS-GVO für den allgemeinen Einsatz von PIMS als Stellvertreter, was eine entsprechende Normierung in künftigen Datenschutzregelungen wünschenswert macht.[71]

6.2.2 PIMS für sachgleiche Datenverarbeitungen

Weniger problematisch ist die Nutzung von PIMS für gleichartige Datenverarbeitungsvorgänge. Für (wohl auch) im Metaverse relevante Trackingverfahren wie z.B. Cookies ist gem. § 3 Abs. 1 der Einwilligungsverwaltungsverordnung (EinwV) die Einführung von PIMS möglich. So könnten etwa Cookies, von deren technischer Relevanz für Metaverseanwendungen bis auf Weiteres auszugehen ist, im Falle des Ablaufes ihrer Gültigkeitsdauer durch die erneute Übermittlung der gültigen Einwilligung „erneuert" werden. Die EinwV setzt § 26 Abs. 1 TDDDG um, wonach Dienste zur Verwaltung von Einwilligungen nach § 25 Abs. 1 TDDDG anerkannt werden können. Die Voraussetzungen an die Einwilligung nach § 25 Abs. 1 TDDDG richten sich weiterhin nach der DS-GVO.[72]

Lediglich die anschließende Verwaltung der Einwilligung kann von einem gem. §§ 8 ff. EinwV anerkannten Dienst übernommen werden, d.h. dass dieser die getroffenen Einstellungen des Endnutzers speichert und dem jeweiligen Digitale-Dienste-Anbieter bei „jeder weiteren Inanspruchnahme des Dienstes" übermittelt (§ 3 Abs. 1 EinwV).[73] Mit anderen Worten nimmt der anerkannte Dienst dem Nutzer „nur" die erneute Übermittlung einer gültigen Einwilligung ab. In Hinblick auf das oben skizzierte Problem

70 *EDSB*, Stellungnahme des EDSB zu Systemen für das Personal Information Management, 2016.

71 S. ausführlicher *Büning/Meyer*, PIMS und das Metaverse: Ein Weg aus dem „Einwilligungs-Banner-Dschungel"? (im Erscheinen).

72 Aufgrund des Umsetzungscharakters des § 25 Abs. 1 TDDDG von Art. 5 Abs. 3 ePrivacy-RL, welcher für die Voraussetzungen auf die DS-RL verweist, die gem. Art. 94 Abs. 2 S. 1 DS-GVO von der DS-GVO abgelöst wurde.

73 Ausführlich *Hunter u.a.*, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, 603 (605); *Jandt*, in: Jandt/Steidle, Datenschutz im Internet, 2025, Kap. IV, Rn. 122 ff.; *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7

um die Dynamik in Bezug auf die datenschutzrechtlich Verantwortlichen und die Verarbeitungszwecke schafft die EinwV keinen echten Mehrwert, da die gespeicherte Einwilligung nur dann noch gültig ist, wenn der Verarbeitungsvorgang gänzlich unverändert ist, also sachgleich mit dem erstmaligen ist.

6.2.3 PIMS für bereichsmäßige Einwilligungen (Broad-Consent)

Um den besonders dynamischen Datenverarbeitungskontexten aufgrund wechselnder datenschutzrechtlicher Verantwortlicher zu begegnen, bedarf es eines ebenso dynamischen Einwilligungsmechanismus. PIMS müssen nicht nur eine bereits erteilte Einwilligung des Nutzers in sachgleichen Verarbeitungsprozessen neu übermitteln, sondern auch in neue Verarbeitungskontexten gegenüber neuen Verantwortlichen eine interessengerechte rechtskonforme Einwilligung erteilen können. Nur dann kann es gelingen, den Abnutzungserscheinungen bisheriger Instrumente Abhilfe zu schaffen. Ein rechtlicher Ansatzpunkt könnte dabei eine bereichsbezogene Einwilligung darstellen, angelehnt an den Rechtsgedanken aus ErwG 33 DS-GVO, der den sogenannten Broad-Consent für wissenschaftliche Forschungszwecke erlaubt. Dabei wird eine allgemeine Einwilligung für einen bestimmten Verarbeitungsbereich erteilt, während konkrete Verarbeitungsdetails zum späteren Zeitpunkt durch eine Instanz – in den Fällen der medizinischen Forschung etwas das Krankenhaus, dass die Patientendaten erhoben hat – spezifiziert werden können.

Ob dieser Ansatz schon grundsätzlich auf kommerzielle Datenverarbeitungen übertragbar ist, bleibt ungeklärt.[74] Erschwerend hinzu kommt der Umstand, dass es im originären Sinne des Broad-Consent lediglich um Spezifikationen der Zwecke der Datenverarbeitung geht; der Betroffene willigt bei der Erhebung der Daten informiert in die Nutzung der Daten zu Forschungszwecken ein, die spezifische Forschung wird jedoch später durch den Verarbeiter bestimmt (z.B. Verarbeitung zu Zwecken der Forschung an Krebs oder aber Alzheimer). In Metaversekonstellationen ginge es aber häufig nicht nur um eine Zweckspezifikation durch PIMS, sondern zusätzlich um eine Verantwortlichenauswahl. Selbst wenn unterstellt würde, dass

DS-GVO, Rn. 34; *Klink-Straub/Straub*, Und bist du nicht willig, so brauch' ich … PIMS, ZD-Aktuell 2024, 01820.

74 Allgemein *Specht-Riemenschneider u.a.*, Die Datentreuhand, MMR-Beilage 2021, 25 (41 ff.).

PIMS in kommerziellen Datenverarbeitungen zu Zweckspezifikationen eingesetzt werden dürften, würde dem Ausgangsproblem der besonderen Verantwortlichendynamik im Metaverse damit nur bedingt Abhilfe geschaffen werden können. Resümierend lässt sich mithin statuieren, dass PIMS technisch große Vorteile bringen könnten, wenn sich sowohl die datenschutzrechtliche Information als auch die Einwilligung damit automatisieren bzw. auslagern ließen. Aus rechtlicher Perspektive ist wenigstens eine effiziente Umsetzung dieser Systeme jedoch (noch) unzulässig.[75]

7. Fazit

Privatheitsfreundliches Design kann erheblich zum Schutz von personenbezogenen Daten und Persönlichkeitsrechten beitragen. Das Konzept „Privacy by Design" ermöglicht es, Datenschutz- und Persönlichkeitsrechte von Anfang an in die Gestaltung virtueller Welten zu integrieren. Dies ist besonders im Metaverse relevant, wo durch immersive Technologien neue Bedrohungsszenarien wie virtuelle Belästigung, Social Bots und besonders intensive Datenerhebung entstehen. Designmaßnahmen können helfen, diese Risiken zu minimieren und eine sicherere digitale Umgebung zu schaffen. Besonders geeignete Designstrategien sind solche, die sowohl technisch wirksam als auch für Nutzer intuitiv bedienbar sind. Weniger geeignete Designlösungen sind solche, die entweder ineffektiv sind oder von den Nutzern als störend empfunden werden. Insbesondere im Bereich des Datenschutzes zeigte sich, dass klassische Einwilligungsmechanismen, wie sie etwa in Cookie-Bannern üblich sind, auf alte Probleme wie Abnutzungserscheinungen treffen, auch wenn sie in neuem Gewand, wie einem virtuellen Assistenten mit Chat-Funktion, präsentiert werden. Hinzu kommen weitere, metaversespezifische Probleme. Hier sehen sich designbasierte Lösungen rechtlichen Hürden gegenüber, denen ggf. nur regulatorisch – z.B. durch Rechtsgrundlagen für bestimmte Strategien wie Personal Information Management Systems (PIMS) – abgeholfen werden kann.

75 Ein rechtsdogmatischer Vorschlag bei *Büning/Meyer*, PIMS und das Metaverse: Ein Weg aus dem „Einwilligungs-Banner-Dschungel"? (im Erscheinen).

Literatur

Abraham, Melvin; Saeghe, Pejman; Mcgill, Mark und Khamis, Mohamed (2022): Implications of XR on Privacy, Security and Behaviour: Insights from Experts. *Nordic Human-Computer Interaction Conference*, 30, S. 1-12. https://doi.org/10.1145/3546155.3546691

Accenture (2022): Technology Vision 2022, Meet Me in the Metaverse, The continuum of technology and experience, reshaping business, S. 1-96.

Adams, Devon; Bah, Alseny; Barwulor, Catherine; Musabay, Nureli; Pitkin, Kadeem und Redmiles, Elissa M. (2018): Ethics emerging: the story of privacy and security perceptions in virtual reality. *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, S. 443-458.

Awadallah, Abeer M.; Damiani, Ernesto; Zemerly, Jamal und Yeun, Chan Yeob (2023): Identity Threats in the Metaverse and Future Research Opportunities. *2023 IEEE International Conference on Business Analytics for Technology and Security (ICBATS)*, S. 1-6. https://doi.org/10.1109/ICBATS57792.2023.10111122

Bender-Paukens, Leonie; Werry, Susanne (2023): Datenschutz im Metaverse. *Zeitschrift für Datenschutz*, S. 127-131.

Benrimoh, David; Chheda, Forum D. und Margolese, Howard C. (2022): The Best Predictor of the Future – the Metaverse, Mental Health, and Lessons Learned From Current Technologies, *JMIR Mental Health*, 9(10), S. 1-9. https://doi.org/10.2196/40410

Botta, Jonas (2021): Delegierte Selbstbestimmung? PIMS als Chance und Risiko für einen effektiven Datenschutz. *Multimedia und Recht*, S. 946-951.

Büning, Felix; Meyer, Markus (2025): PIMS und das Metaverse: Ein Weg aus dem "Einwilligungs-Banner-Dschungel". (im Erscheinen).

Chalfin, Aaron; Hansen, Benjamin; Lerner, Jason und Parker, Lucie (2022): Reducing Crime Through Environmental Design: Evidence from a Randomized Experiment of Street Lighting in New York City. *Journal of Quantitative Criminology*, 38, S. 127-157. https://doi.org/10.1007/s10940-020-09490-6

Davis, Alanah; Murphy, John; Owens, Dawn; Khazanchi, Deepak und Zigurs, Ilze (2009): Avatars, People, and Virtual Worlds: Foundations for Research in Metaverses. *Journal of the Association for Information Systems*, 10(2), S. 91-117. https://doi.org/10.17705/1jais.00183

Dincelli, Ersin und Yayla, Alper (2022): Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective. *The Journal of Strategic Information Systems*, 31(2), 101717, S. 1-22. https://doi.org/10.1016/j.jsis.2022.101717

Dionisio, Jahn David N.; Bruns III, William G. und Gilbert, Richard (2013): 3D Virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys*, 45(3), 34, S. 1-38. https://doi.org/10.1145/2480741.2480751

Di Pietro, Roberto und Cresci, Stefano (2021): Metaverse: Security and Privacy Issues. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, S. 281-288. https://doi.org/ 10.1109/TPSISA52974.2021.00032

Dolata, Mateusz und Schwabe, Gerhard (2023): What is the Metaverse and who seeks to define it? Mapping the site of social construction. *Journal of Information Technology*, 38(3), S. 239-266. https://doi.org/10.1177/02683962231159927

Dwivedi, Yogesh K.; Kshetri, Nir; Hughes, Laurie; Rana, Nripendra P.; Baabdullah, Abdullah M.; Kar, Arpan Kumar; Koohang, Alex; Ribeiro-Navarrete, Samuel; Belei, Nina; Balakrishnan, Janarthanan; Basu, Sriparna; Behl, Abhishek; Davies, Gareth H.; Dutot, Vincent; Dwivedi, Rohita; Evans, Leighton; Felix, Reto; Foster-Fletcher, Richard; Giannakis, Mihalis; Gupta, Ashish; Hinsch, Chris; Jain, Animesh; Patel, Nina Jane; Jung, Timothy; Juneja, Satinder; Kamran, Qeis; Mohamed AB, Sanjar; Pandey, Neeraj; Papagiannidis, Savvas; Raman, Ramakrishnan; Rauschnabel, Philipp A.; Tak, Preeti; Taylor, Alexandra; tom Dieck, M. Claudia; Viglia, Giampaolo; Wang, Yichuan und Yan, Meiyi (2023): Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. *Information Systems Frontiers*, 25(5), S. 2071-2114. https://doi.org/10.1007/s10796-023-10400-x

EDSB (2016): Stellungnahme des Europäischen Datenschutzbeauftragten zu Systemen für das Personal Information Management (PIM): Hin zu einer intensiveren Einbindung der Nutzer in das Management und die Verarbeitung personenbezogener Daten, Brüssel: Europäischer Datenschutzbeauftragter. URL: https://www.edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_de.pdf (besucht am 28.02.2025).

Europäische Kommission (2025): Datenschutz und Privatsphäre in virtuellen Welten. URL: https://digital-strategy.ec.europa.eu/policies/virtual-worlds-data-protection-privacy (besucht am 12.05.2025).

Falchuk, Ben; Loeb, Shoshana und Neff, Ralph (2018): The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine*, 37(2), S. 52-61. https://doi.org/10.1109/MTS.2018.2826060

Fernandez, Carlos Bermejo und Hui, Pan (2022): Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse. *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, S. 272-277. https://doi.org/10.1109/ICDCSW56584.2022.00058

Fotios, Steve A.; Robbins, Chloe J. und Farall, Stephen (2021): The Effect of Lighting on Crime Counts. *Energies*, 14(14), 4099, S. 1-14. https://doi.org/10.3390/en14144099

Franks, Mary-Ann (2017): The Desert of the Unreal: Inequality in Virtual and Augmented Reality. *UC Davis Law Review*, 51(2), S. 499-538.

Freeman, Gou; Zamanifard, Samaneh; Maloney, Divine und Acena, Dane (2022): Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1), 85, S. 1-30. https://doi.org/10.1145/3512932

Gartner (07. Februar 2022): Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026, gartner.com. URL: https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026 (besucht am 28.02.2025).

Gerpott, Torsten J. (2020): Datenschutzerklärungen – Materiell fundierte Einwilligungen nach der DS-GVO. Empirischer Forschungsstand und Verbesserungsfelder. *Multimedia und Recht*, S. 739-744.

Happa, Jassim; Steed, Anthony und Glencross, Mashhuda (2021): Privacy-certification standards for extended-reality devices and services. *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, S. 397-398. https://doi.org/10.1109/VRW52623.2021.00085

Hunter, Julian; Ebert, Andreas und Spieker genannt Döhmann, Indra (2024): Informationspflichten und Einwilligung bei der Nutzung von PIMS: Probleme und Potenziale der Einwilligungsverwaltung de lege lata. *Zeitschrift für Datenschutzrecht*, S. 603-610.

Jandt, Silke und Steidle, Roland (Hrsg.) (2025): Datenschutz und Internet. 2. Auflage. Baden-Baden: Nomos.

Kang, Giluk; Koo, Jahoon und Kim, Young-Gab (2024 Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective. *IEEE Communications Magazine*, 62(1), S. 148-154. https://doi.org/10.1109/MCOM.014.2200620

Kern, Michael (2024): Die Verwendung von Social Bots – Transparenzpflichten gemäß Medienstaatsvertrag und KI-VO sowie deren Umsetzung in virtuellen Welten. *KI und Recht*, S. 94-99.

Kettner, Sara Elisa; Thorun, Christian und Spindler, Gerald (2020): Innovatives Datenschutz-Einwilligungsmanagement: Abschlussbericht im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz, Berlin: BMJV. URL: https://www.conpolicy.de/data/user_upload/Studien/ConPolicy_Innovatives_Einwilligungsmanagement.pdf (besucht am 28.02.2025).

Kettner, Sara Elisa; Thorun, Christian und Vetter, Max (2018): Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz. Vorgelegt bei der: Bundesanstalt für Landwirtschaft und Ernährung (BLE), Bonn. URL: https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (besucht am 05.05.2025).

Klar, Manuel; Wegmann, Simon Clemens und Galandi, Michaela (2022): Datenschutz im Metaverse. *Betriebsberater*, S. 2691-2696.

Klink-Straub, Judith und Straub, Tobias (2024): Und bist du nicht willig, so brauch‘ ich … PIMS – Entwurf der Einwilligungsverwaltungsverordnung nach § 26 TDDDG. Newsdienst ZD-Aktuell, 01820.

Kroschwald, Steffen (2023): Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften: Schutz, Selbstbestimmung und Teilhabe „by Design“ vor dem Hintergrund des Art. 25 DS-GVO und dem KI-Verordnungsentwurf. *Zeitschrift für Digitalisierung und Recht*, S. 1-22.

Kühling, Jürgen; Sauerborn, Cornelius (2022): PIMS vs. Einwilligung vs. Browsereinstellungen. *Zeitschrift für Datenschutz*, S. 596-599.

Maloney, Divine; Zamanifard, Samaneh und Freeman, Guo (2020): Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality. *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology*, 25, S. 1-9. https://doi.org/10.1145/3385956.3418967

Marloth, Maria; Chandler, Jennifer und Vogeley, Kai (2020): Psychiatric Interventions in Virtual Reality: Why We Need an Ethical Framework. *Cambridge Quarterly of Healthcare Ethics*, 29(4), S. 574-584. https://doi.org/10.1017/S0963180120000328

McStay, Andrew (2023): The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy and Technology*, 36, 13, S. 1-26. https://doi.org/10.1007/s13347-023-00613-y

Mello, Manuel; Dupont, Lennie; Engelen, Tahnée; Acciarino, Adriano; de Borst, Aline und de Gelder, Beatrice (2022): The influence of body expression, group affiliation and threat proximity on interactions in virtual reality. *Current Research in Behavioral Sciences*, 3, 100075, S. 1-8. https://doi.org/10.1016/j.crbeha.2022.100075

Mitre-Becerril, David; Tahamont, Sarah; Lerner, Jason und Chalfin, Aaron (2022): Can deterrence persist? Long-term evidence from a randomized experiment in street lighting. *Criminology & Public Policy*, 21(4), S. 865-891. https://doi.org/10.1111/1745-9133.12599

Nüske, Niclas; Olenberger, Christian; Rau, Daniel und Schmied, Fabian (2019): Privacy Bots. Digitale Helfer für mehr Transparenz im Internet. *Datenschutz und Datensicherheit*, S. 28-32.

Papagiannidis, Savvas; Bourlakis, Michael und Li, Feng (2008): Making real money in virtual worlds: MMORPGs and emerging business opportunities, challenges and ethical implications in metaverses. Technological Forecasting and Social Change, 75(5), S. 610-622. https://doi.org/10.1016/j.techfore.2007.04.007

Roblox (22. Januar 2025): Roblox-Datenschutz- und Cookie-Richtlinie, roblox.com URL: https://en.help.roblox.com/hc/article_attachments/20961293100820 (besucht am 28.02.2025).

Rosenblat, Mariana Olaizola (2023): Reality Check: How to Protect Human Rights in the 3D Immersive Web, Ney York City: NYU Stern Center for Business and Human Rights. URL: https://bhr.stern.nyu.edu/wp-content/uploads/2023/09/NYUCBHRMetaverse_Sep5ONLINEFINALCOVER1ADA.pdf (besucht am 28.02.2025).

Ruiz Mejia, Jose M. und Rawat, D. B. (2022): Recent Advances in a Medical Domain Metaverse: Status, Challenges, and Perspective. *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, S. 357-362. https://doi.org/10.1109/ICUFN55119.2022.9829645

Schuchardt, Lisa-Marie (2025): Die (ferne) Zukunft der Cookie-Einwilligung: PIMS und der Weg zu datenschutzfreundlichen Lösungen, *Datenschutz-Berater*, S. 103-106.

Simitis, Spiros; Hornung, Gerrit und Spiecker genannt Döhmann, Indra (Hrsg.) (2025): Datenschutzrecht. 2. Auflage. Baden-Baden: Nomos.

Smith, Carl H.; Molka-Danielsen, Judith; Rasool, Jazz und Webb-Benjamin, Jean-Brunel (2023): The World as an Interface: Exploring the Ethical Challenges of the Emerging Metaverse. *Proceedings of the 56th Hawaii International Conference on System Sciences*, S. 6045-6054. https://hdl.handle.net/10125/103367

Specht-Riemenschneider, Louisa; Blankertz, Aline; Sierek, Pascal; Schneider, Ruben; Knapp, Jakob und Henne, Theresa (2021 Die Datentreuhand: Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle. *Multimedia und Recht Beilage*, S. 25-48.

Spindler, Gerald und Förster, Lydia (2023): Privacy-compliant design of Cookie Banners according to the GDPR. *JIPITEC*, 14(1), S. 2-33.

Steege, Hans und Chibanguza, Kuuya J. (Hrsg.) (2023): Metaverse: Rechtshandbuch. Baden-Baden: Nomos.

Stephenson, Neal (1992): Snow Crash. New York City: Bantam Books.

Tricomi, Pier Paolo; Nenna, Federica; Pajola, Luca; Conti, Mauro und Gemberini, Luciano (2023): You Can't Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality. *IEEE Access*, 11, S. 9859-9875. https://doi.org/10.1109/ACCESS.2023.3240071

Venugopal, Jothi Prakash; Subramanian, Arul Antran Vijay und Peatchimuthu, Jegathesh (2023): The realm of metaverse: A survey. *Computer Animation and Virtual Worlds*, 34(5), S. 1-28. https://doi.org/10.1002/cav.2150

Vladimirov, Ivaylo; Nenova, Maria; Nikolova, Desislava und Terneva, Zornitsa (2022): Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey. *2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, S. 1-4. https://doi.org/10.1109/ICEST55168.2022.9828791

Wang, Cheng Yao; Sriram, Sandhya und Stevenson Won, Andrea (2021): Shared Realities: Avatar Identification and Privacy Concerns in Reconstructed Experiences. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 337, S. 1-25. https://doi.org/10.1145/3476078

Wiederhold, Brenda (2022): Sexual Harassment in the Metaverse. Cyberpsychology, Behavior, and Social Networking, 25(8), S. 479-548. https://doi.org/10.1089/cyber.2022.29253.editorial

Xie, Runjie; Kirchner-Krath, Jeanine und Morschheuser, Benedikt (2024): Towards an Ethical Metaverse: A Systematic Literature Review on Privacy Challenges. *Proceedings of the 32nd European Conference on Information Systems (ECIS 2024),6.*