Metaverse: Datenschutz in der digitalen Welt

Das Metaverse wird aktuell als die nächste Iteration des Internets gehandelt. Eine genaue Definition, was unter dem Begriff „Metaverse“ überhaupt zu verstehen ist und wie dieses konkret technisch ausgestaltet sein wird, steht dabei noch gar nicht fest. Einigkeit besteht jedoch darüber, dass das Metaverse einen dezentralen, virtuellen, hochgradig interaktiven und transaktionsgetriebenen Raum mit fließenden Verknüpfungen zur realen Welt darstellen wird. Neue Technologien im Bereich „Extended Reality“ sowie die Einführung von „Digital Twins“ – digitalen Repräsentanzen realer Assets – bieten völlig neue Formen der Interaktion und Auswertung anfallender Daten. Schon bei einer 20-minütigen Nutzung eines VR-Headsets können bis zu zwei Millionen Datenpunkte erfasst werden; viele davon biometrisch und damit besonders schützenswert. Dabei ist eine der großen rechtlichen Herausforderungen, das Metaverse mit bestehenden Datenschutzvorschriften, insbesondere denen der Datenschutz-Grundverordnung (DSGVO), in Einklang zu bringen.

Datenschutzrechtliche Verantwortlichkeit

Die DSGVO ist auch im Metaverse anwendbar. Ihre Pflichten treffen Verantwortliche, die in der EU niedergelassen sind oder personenbezogene Daten, die in der EU gewonnen wurden, verarbeiten. Doch die Unsicherheiten beginnen schon bei der Beantwortung der grundsätzlichen Frage nach der datenschutzrechtlichen Verantwortlichkeit. Gemäß Artikel 4 Nr. 7 der DSGVO ist Verantwortliche:r die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. So wie das Internet derzeit gestaltet ist, kann die Verantwortlichkeit relativ einfach durch die Zuordnung einer Website zu einem bzw. einer Betreiber:in bestimmt werden. Mit Aufrufen einer neuen Website wird der Verantwortungsbereich des Betreibers bzw. der Betreiberin der alten Seite verlassen und der des Betreibers bzw. der Betreiberin der nächsten Seite betreten. Derartig klare Abgrenzungen werden im Metaverse jedoch kaum denkbar sein und sind mit der Vorstellung einer immersiven virtuellen Welt mit nahtlosen Übergängen zwischen verschiedensten Angeboten nicht vereinbar. Eine Anknüpfung an die „Eigentümer:innen“ virtueller Räumlichkeiten, in welchen sich die Avatare von Nutzer:innen aufhalten, ist ein möglicher Ansatz. Allerdings wird es im Metaverse auch „öffentliche“ Bereiche wie Plätze und Wege geben, die keinem bzw. keiner einzelnen Anbieter:in zuzuordnen sind und an denen die virtuellen Shops und Präsenzen angrenzen. Wie werden diese zu behandeln sein? Sind die daran angrenzenden Anbieter:innen gemeinsam Verantwortliche? Oder gibt es eine:n virtuelle:n „Infrastrukturanbieter:in“, der bzw. die für Datenverarbeitungen in diesen Bereichen verantwortlich ist? Die dezentrale und nahtlose Ausgestaltung des Metaverse wird bei der Bestimmung datenschutzrechtlicher Rollen unter der DSGVO noch zu einigem Kopfzerbrechen führen.

Datenschutzrechtliche Informationspflichten

Eine Frage eher praktischer Natur betrifft die Erfüllung von Informationspflichten nach Artikel 13 und 14 der DSGVO. Demnach müssen Verantwortliche im Vorfeld über die Einzelheiten der Datenverarbeitung aufklären. Würde man die bisherige Praxis ausführlicher Datenschutzerklärungen ins Metaverse übertragen, würde dies im wahrsten Sinne des Wortes zu „walls of text“ führen, die sich äußerst störend auf die Immersion auswirken und die User-Experience nachhaltig beeinträchtigen würden. Hier könnte der bisher kaum beachtete Artikel 12 Abs. 7 der DSGVO zum Tragen kommen. Dieser sieht die Verwendung standardisierter Bildsymbole vor. Dadurch lässt sich die Menge an notwendigem Text reduzieren. Durch Interaktion mit dem jeweiligen Icon können Nutzer:innen

zusätzliche Informationen zu der kenntlich gemachten Datenverarbeitung erlangen.

Marketing, sensible Daten & Einwilligungen

Gerade bei der Einbindung von Extended Reality-Devices – also Geräten, wie Headsets und anderen Sensoren, die unter anderem geeignet sind, Mimik, Gestik und sonstige Bewegungen des Nutzers bzw. der Nutzerin auf seinen bzw. ihren Avatar zu übertragen – werden Unmengen biometrischer Daten in Echtzeit verarbeitet, die sogar auf medizinische Indikationen schließen lassen können. Optische Sensoren erfassen die Umgebung des Nutzers bzw. der Nutzerin – in der Regel die eigene Wohnung – und Mikrofone übermitteln jedes gesprochene Wort. Die Erfassung dieser Daten wird völlig neue Möglichkeiten für Profiling- und Trackingtechnologien bieten. So lässt sich etwa aus der Pupillenerweiterung herauslesen, dass dem bzw. der Nutzer:in betrachtete Anzeigen oder Produkte gefallen, ohne, dass er bzw. sie dies bewusst steuern kann. Während die Nutzung biometrischer und anderer sensibler Daten ohnehin regelmäßig eine ausdrückliche Einwilligung voraussetzen, stellt sich die Frage, ob eine umfangreiche Auswertung und Nutzung weiterer Daten, die User unbewusst preisgeben, zu Marketingzwecken auf Grundlage eines berechtigten Interesses erfolgen darf oder ebenfalls nur auf Grundlage einer Einwilligung. Und wie sollten Einwilligungen ausgestaltet werden? Eine konkludente Einwilligung im Onlinebereich kann nicht ohne Weiteres angenommen werden. Es bedarf einer ausdrücklichen Willensbekundung des Nutzers bzw. der Nutzerin. Das bloße Weiternutzen einer Website trotz Cookie-Hinweises oder das Akzeptieren vorausgefüllter Checkboxen genügen nicht. Entsprechend dürfte auch dem bloßen Betreten einer Metaverse-Präsenz, welche einwilligungsbedürftige Verarbeitungen auslöst, kein entsprechender Erklärungsinhalt zu kommen. Doch genügt hier vielleicht schon ein Kopfnicken des Avatars als Einwilligung?

Drittlandtransfer

Während die zuvor dargestellten Schwierigkeiten großteils durch Gestaltungen technischer Art lösbar sind und sich, wie im Bereich von Cookie-Bannern, voraussichtlich eine immer klarere Linie der Rechtsprechung an die genauen Anforderungen herauskristallisieren wird, ist das wesentlich größere Problem der Drittlandtransfers der Daten. Auf Grund der um ein Vielfaches erhöhten Anzahl erhobener Daten und der ständigen Datenübermittlung bei der Nutzung des Metaverse, erscheint ein Rückgriff auf die bestehenden Transferinstrumente nicht immer zielführend. Insbesondere die Standardvertragsklauseln zum internationalen Datentransfer unterliegen noch dem Grundgedanken der aktuellen Ausgestaltung des Internets, d.h. dass es jeweils vorab definierbare Datenexporteure und Datenimporteure sowie Datenverarbeitungen gibt. Doch sollte es sich beim Metaverse tatsächlich um eine dezentrale Plattform handeln, ist Teil des Reizes dieser Plattform, dass sich die Nutzer:innen ständig im spontanen Austausch ihrer Daten mit Dritten in ihrer virtuellen Umgebung befinden. Welche Daten von wem und an wen zu welchen Zwecken übermittelt werden, lässt sich vorab nur schwer bestimmen – außer in einem kontrollierten Umfeld, in welchem die Handlungsmöglichkeiten von Nutzer:innen auf ein vorhersehbares Maß reduziert werden. Doch dies würde der Vorstellung einer wahren virtuellen Welt entgegenstehen.

Fazit

Schon die Betrachtung dieser kleinen Auswahl naheliegender datenschutzrechtlicher Fragestellungen zeigt, dass das Recht in seiner jetzigen Form noch nicht für den Einsatz in dezentralen virtuellen Welten ausgelegt ist. Es wird eine Herausforderung für alle Beteiligten, einen angemessenen Ausgleich zwischen Nutzerfreundlichkeit und Immersion auf der einen Seite sowie der Erfüllung datenschutzrechtlicher Vorgaben auf der anderen Seite zu

finden. Durch neu entwickelte smarte technische und rechtliche Methoden ist die Vereinbarkeit einer virtuellen Welt, die der Vielfalt unserer Realität in nichts nachsteht, mit dem geltenden Datenschutzrecht aber denkbar – auch wenn künftige regulatorische Anpassungen unvermeidlich sein werden.

Ansprechpartner:

Francois Heynike, LL.M. (Stellenbosch)
Tel: +49-69-951195770
fheynike@kpmg-law.com