EU: Privacy and security concerns in the metaverse

By **Danique Knibbeler** Associate
danique.knibbeler@nautadutilh.com
NautaDutilh N.V., Amsterdam

By **Max Mohrmann** Associate
max.mohrmann@nautadutilh.com
NautaDutilh N.V., Amsterdam

By **Sarah Zadeh** Associate
sarah.zadeh@nautadutilh.com
NautaDutilh N.V., Amsterdam

In light of an increasing interest and engagement with the metaverse, the question arises whether current laws and regulations adequately address the processing activities within it. Danique Knibbeler, Max Mohrmann, and Sarah Zadeh, from NautaDutilh N.V., discuss key considerations in relation to the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and assess other laws, regulations, and legal proposals and their applicability, whilst also exploring potential security risks resulting from the interactions in the metaverse.

Introduction

Initially mainly a phenomenon in the gaming industry, the metaverse - a virtual world in which end-users can interact - has gained increased traction in the past few years. McKinsey & Company reported that technology companies, venture capitalists, private equity funds, start-ups, and established brands are seeking opportunities to capitalise on the metaverse, by making metaverse investments of more than $120 billion in the first five months of this year alone[1].

There are several reasons that can explain the increased interest and these significant investments. For example, more and more consumers have become interested in exploring the metaverse, largely driven by gaming. In addition, the metaverse is becoming more technologically advanced through new applications, interoperability with different smart devices, and an improved infrastructure.

These developments also present risks. As the metaverse is data-driven, the development and further use of the metaverse implies the collection of an extensive amount of personal data (Article 4 (1) of the GDPR), such as physiological responses, facial movements, gestures, brainwave patterns and behavioural patterns. In the metaverse, wearables and other smart devices and platforms will need to be connected, which brings security risks, but also risks with respect to the processing of personal data, especially in regards to the unique profiles of end-users. This poses the question whether current laws and regulations adequately address the processing activities in the metaverse, and whether additional guidance should be provided, or existing laws should be updated. This article elaborates on the key concerns in relation to the GDPR; the applicability of other laws and regulations and legal proposals, such as the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC ('the Draft DSA')[2] and the Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data ('the Draft Data Act')[3]; and potential security risks.

What is the metaverse?

The term metaverse - a combination of the Greek word 'meta' and the word 'universe' - was initially coined by the science-fiction author Neal Stephenson in his novel 'Snow Crash' (1992), and referred to a virtual, parallel world.

The Council of the European Union ('the Council') described it as 'an immersive and constant virtual 3D world where people interact through an avatar to enjoy entertainment, make purchases and carry out transactions with crypto-assets, or work without leaving their seat'[4]. Even though the metaverse refers to a 'virtual 3D world', it is not mandatory to use 3D-devices for a virtual world to be considered a 'metaverse'. It depends on the metaverse provider and the device how the metaverse can be accessed and experienced. Depending on the platform, the metaverse can be accessed via technologically more advanced devices, such as VR-goggles, or more traditional devices, such as a 2D game console or desktop.

Therefore, this article distinguishes between two kinds of metaverses:

- a centralised blockchain-based metaverse (e.g. Earth2) or a decentralised blockchain-based metaverse (e.g. Decentraland, The Sandbox), which we chose to coin as an 'advanced metaverse'; and
- a more centralised metaverse (e.g. Second Life, Grand Theft Auto Online), which we chose to coin as a 'traditional metaverse'.

Key concerns in relation to the GDPR

As personal data will be processed by all kinds of technical applications and devices, the regulation of personal data is necessary to safeguard the privacy of the individual and the integrity of personal data. The question arises whether the current data protection framework, such as that drawn up by the GDPR, is sufficient to regulate the processing of personal data within the metaverse. For instance, it might be difficult to determine the territorial application of the GDPR.

The application of the GDPR depends on the location of the end-user when their personal data is processed, not on their residence or citizenship (Article 3 of the GDPR). But what is the location of the end-user within the metaverse? Is this the physical location of the end-user controlling the avatar, or the avatar itself, or the location of the relevant server? In addition, the GDPR restricts data transfer to third countries (Chapter V of the GDPR), but the metaverse consists of interconnected digital world where no borders exist.

Regarding the applicability of the GDPR the following key concerns need to be addressed:

Lack of clarity on qualifying (joint) controllers or (sub-)processors

The metaverse is a web of different organisations and relationships, with interchangeable roles, responsibilities, and liabilities. In that regard, it may be difficult to determine who the (joint) controllers (Article 4(7) of the GDPR) and/or (sub-)processors (Article 4(8) of the GDPR) are. Questions may arise, such as who is required to assess a valid ground for processing data (Article 6 of the GDPR), and who is obliged to report a data breach (Articles 33 and 34 of the GDPR). As long as these roles are not clearly defined, the risk of incorrect implementation of compliance obligations increases.

Data sharing within the metaverse

Given the nature of the metaverse, namely the interoperability between different devices, platforms, and environments, large amounts of personal data are shared between parties. Prior to the sharing of such personal data, the parties concerned should conclude appropriate data sharing agreements, which should meet the requirements set out in the GDPR. Any data processing agreement concluded between a processor and a controller must comply with the requirements as set out in Article 28(3) of the GDPR, whilst an arrangement between joint controllers must comply with the requirements in accordance with Article 26 of the GDPR. Even though the GDPR does not mention any obligation to conclude a (written) agreement regarding the sharing of personal data between controllers, such a (written) agreement is advisable[5]. Regarding the data sharing arrangement between (joint) controllers, particular attention should be given to determining the responsibilities regarding the exercise of data subject rights (Articles 15 to 22 of the GDPR) and the responsibilities to provide information to the individual users (Articles 12 and 13 of the GDPR). Due to the different parties involved and the large amount of personal data that is being processed, we expect that properly informing the end-users about their data subject rights and determining the responsibilities in relation to the exercise of data subject rights might impose further challenges.

In addition, the possibility for end-users to link with, and switch between, metaverses requires the platform providers to enable data portability and interoperability between other metaverses, in order to avoid a 'vendor lock-in', which means that end-users are dependent of a specific metaverse environment and are not able to easily re-use their personal data. This right to data portability under the GDPR (Article 20) only applies if the processing of personal data is based on the processing ground of consent (Articles 4(11) and 6(1)(a)) or contract (Article 6(1)(b)) and only for that data that they have provided to the controller. However, we recommend that organisations enable this right by default in every metaverse, regardless of the processing ground. We believe that the exercise of data portability strengthens interoperability within the metaverse and will further strengthen the autonomy of the end-user.

Published by OneTrust DataGuidance™ | May 2022

Ground for processing: consent?
Consent as processing ground must be informed, freely given, specific, and unambiguous (Articles 4(11) and 6(1) of the GDPR). Explicit consent is required when processing special categories of data (Article 9(1)(a) of the GDPR). The component 'free' entails that there must be a genuine choice and control for the individual. The consent is not freely given if the individual feels compelled to give consent, if they will suffer negative consequences if they do not give consent, or if in fact they have no alternative. It is reported that, within 20 minutes, in a virtual reality, 2 million unique recordings of body language (such as eye movements, face expressions, and skin temperature) are processed. The collection of such large amounts of personal data within a short period raises issues regarding the transparency of the personal data that is being processed, with the consequence that the end-user is not informed properly, which complicates obtaining informed, explicit, and specific consent.

In addition, if different purposes for processing are merged and the individual is not able to consent for each purpose separately, but only for a bundle of purposes, there is a lack of freedom and thus the consent is presumed not to be freely given. Asking for separate consent is expected to be difficult due to the large amounts of data and affects its user-friendliness.

Also, explicit consent may frustrate the very objective of the metaverse, which is to provide an interconnected network of digital worlds in which platforms, devices, and people are seamlessly connected. The requirement of asking explicit consent multiple times in a short period would frustrate this objective. Companies should provide transparency about data collection and allow the end-user to consent to specific data collections, rather than consent to a bundle of data sets.

Avatars and their unique profiles: profiling and automated decision-making
Another key concern is the extensive amount of personal data that will be collected in the metaverse; for example real-time tracking of end-users by new technologies that collects eye tracking, emotional reaction, voice interaction, social interaction, touching, and hearing. The combination of these data categories reveals specific personal characteristics and interactions that could create more unique profiles of end-users by means of an avatar. In addition, these unique profiles may also be used for automated decision-making (Article 22 of the GDPR) and/or profiling (Article 4(4) of the GDPR), which can create and perpetuate existing stereotypes and social segregation, e.g. restricting the access of avatars to certain spaces within the metaverse based on their social and emotional interactions, or in combination with, for example, their religious beliefs, sexual orientation, and racial or ethnic origin, which are qualified as special category data under the GDPR (Articles 9(1) and 22(4)). Profiling can also lead to the exclusion of a person from a particular category, or confine a person to a particular category, thus limiting their preferences, whereby their freedom to choose could be undermined. It may even result in physical, material, or immaterial harm, in particular when using unique profiles of certain groups of society, such as minority groups, vulnerable adults, and children.

Other upcoming data regulations in the metaverse

Due to the different types of data processing in and outside of the metaverse, other (upcoming) data regulations will apply besides the GDPR. In response to the increased growth of such new technologies, the European Commission has recently proposed new initiatives that strengthen the existing framework of data regulation. These include the Draft DSA, the Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) ('the Draft DMA')[6], the Digital Governance Act ('DGA')[7], Draft Data Act, and the Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts ('the Draft AI Act')[8]. Although it is uncertain to what extent these will be applicable to the metaverse, the Commission already stated that the Draft DSA and the Draft DMA will provide, in their opinion, the necessary tools to regulate the metaverse[9].

First, the Draft DSA aims to provide a more comprehensive form of protection by requiring restrictions on the use of data, but will also impose limits on target advertising, such as behaviourally targeted advertising to minors, and targeted advertising based on special categories of data, which allow for targeting vulnerable recipients, because of their gender, race or ethnic origin, or disability. The Draft DSA also prohibits so-called 'dark patterns', which are design techniques that push or deceive consumers into decisions that have negative consequences for them.

Second, the Draft DMA lays the focus on core platform services which act as 'gatekeepers' that remedy competition aspects. This proposal effectively bans combining and re-using personal data collected during the use of a service and for the purpose of another service offered by the gatekeeper. However, the Draft DMA simultaneously complements the GDPR's right to (personal) data portability, which stimulates the necessary real-time access and control for end-users in the metaverse.

In addition to the Draft DSA and the Draft DMA, the Draft AI Act will play a key factor in regulating e.g. the end-user unique profile and avatars in the metaverse, as much of their experience will be provided by artificial intelligence ('AI') features that are data-driven. In order to enable such features, such as facial recognition and direct translation of spoken texts, organisations must keep in mind that AI in the metaverse uses and generates high-quality data on a large scale.

Similarly, the DGA and Draft Data Act strive to foster data sharing amongst organisations, which will translate directly into business operations within the metaverse and help facilitate seamless interoperability.

Due to these new laws and regulations, a patchwork of laws is slowly being formed and gaps are being identified between these different laws and regulations, resulting in legal inconsistencies and regulatory uncertainty. For example, the European Data Protection Board ('EDPB') and the European Data Protection Supervisor ('EDPS') have noted that the current Draft Data Act does not distinguish between personal data and non-personal data in defining the scope of the rights of access and the processing of data, which increases the risk that personal data may be processed without the prior knowledge of the individual[10]. In addition, the Draft Data Act does not mention the controller and processor roles in relation to the processing of personal data, and it does not further clarify the interaction with some key provision of the Draft DMA related to data sharing (Articles 6(1)(h) and 6(1)(i))[11]. Furthermore, the Draft AI Act does not explicitly clarify that the GDPR - and other data protection laws, such as the Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the ePrivacy Directive') - will also apply to the processing of any personal data[12]. Such inconsistencies and ambiguities frustrate the creation of an adequate legal framework based on which the metaverse can be further developed.

Security risks

In general, the security risks of the metaverse will depend on the platform, the kind of processing activities, and the interconnected devices that will be used. However, even 'emerging' environments, such as the metaverse and technologically advanced devices, as used within the metaverse, can become subject of 'traditional' cyber attacks, such as hacking, malware, denial-of-service attacks, but also fraud and phishing scams.

Security risks may also occur in relation to the ownership and transactions of digital assets, such as non-fungible tokens and cryptocurrencies, for example digital wallets of end-users have not been secured properly or in case of a scam. Such vulnerabilities pose a serious threat, as maintaining end-user identification is essential to prevent identity theft in the digital world, especially considering the possibility to imitate an end-user's avatar during user-to-user communication.

Due to its interoperability and interconnection, (personal) data that is being stored within the metaverse enabling devices are exchanged real-time. Consequently, however, the security integrity of a single device cannot guarantee data protection when the (personal) data is being transferred to another enabling device.

It is important that platform providers and third parties that offer supporting services or metaverse enabling devices must assess which technical and organisational measures should be taken to assess and mitigate potential risks. Without proper technical and organisational measures to offer adequate protection of these devices, there is an increasing risk that a breach of security will take place, which may lead to accidental or unlawful loss or access to personal data of the metaverse end-users.

The European Parliamentary Research Service emphasised that identity identification built on blockchain will be crucial in this respect, as it is more resistant to cyber attacks, compared to a centralised system and suggested to protect the integrity of the devices used in connection with the metaverse, to build new cybersecurity protocols between platforms[13]. Such protocols should be comparable and add-on to the revised Directive on Security of Network and Information Systems ('NIS2'), which increases EU national cybersecurity capabilities[14], or the proposed cybersecurity resilience act, that focuses on cybersecurity rules for digital products[15]. To ensure a certain standard of security, the European Parliamentary Research Service proposed to implement standard security protocols. However, many of the abovementioned vulnerabilities will also depend on the end-user's ability to identify such threats and adapt accordingly to comply with implemented technical and organisational measures by the platform and device providers, in order to guarantee their own data protection.

Conclusion and general recommendations

In this article, we have addressed the main GDPR concerns, namely the territorial applicability of the GDPR, issues regarding the qualification of roles, data sharing within the metaverse, consent as processing ground, profiling, and automated decision-making. In addition, we have discussed upcoming data regulations that apply on the metaverse, as well as possible security risks.

Based on the current data legislations and proposals, we see room for improvement, namely in providing clarity in relation to the interplay between the different legal frameworks which apply to the metaverse. In addition, due to the use of, and interoperability between, the platforms and devices, the metaverse is prone to security risks and risks with respect to the processing of personal data, especially in regards to the unique profiles of end-users. With regards to the interoperability, we recommend that the involved parties conclude appropriate data sharing agreements, assess potential security risks, and implement appropriate technical and organisational security measures to safeguard the processing of personal data.

Lastly, with regards to transparency, we recommend that the involved parties, irrespective of their role as (joint) controller or processor, inform the end-user in a clear and consistent manner about the processing of personal data that takes place within the metaverse, whilst avoiding that end-users get presented with excessive amount of incomprehensible information by means of privacy statements. Due to the different parties involved and the amounts of personal data that will be processed, transparency about the functionality and the impact of the metaverse remains key.

1. McKinsey & Company: Value Creation in the Metaverse, June 2022, available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf
2. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN
3. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN
4. See at: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf
5. European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 1.0, adopted on 02 September 2020, available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf
6. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN
7. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767
8. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
9. See at: https://www.europarl.europa.eu/doceo/document/E-9-2022-000656-ASW_EN.pdf
10. EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en
12. EDPB-EDPS Joint Opinion 5/2021on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), available at: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
13. See at:: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf
14. See at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
15. See at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-

Published by OneTrust DataGuidance™ | May 2022