Data protection and the metaverse: more of the same or a big challenge?

news
legal,

20 October 2023

In October 2021, Mark Zuckerberg surprised everyone by announcing that Facebook would turn into Meta. At the same time, he unveiled ambitious plans to develop the Metaverse (capitalized if it depends on Meta). In this virtual world, people can communicate, work, play and trade with others. The metaverse is a place where people come together and interact, similar to the real world, with opportunities in e-commerce, gaming, education and healthcare.

But as with any new technology, the rise of the metaverse brings with it concerns, especially in the areas of privacy and data protection. In this blog, we discuss the role of the General Data Protection Regulation (GDPR) in the development of the metaverse.

Who is responsible for data processing?

An important question regarding the metaverse is who is responsible for processing and compliance with GDPR principles. Is it the company that co-develops the metaverse, such as Meta itself? Or is it a company that operates in the metaverse, for example a doctor's office that offers online diagnostic services through the metaverse where sensors collect data such as heart rate and blood pressure?

To answer this question, we need to make a clear distinction between the controller and the processor. The controller determines the purpose and means of processing personal data, while the processor processes data on behalf of the controller. In the doctor's office example, the doctor's office is the controller because they are responsible for collecting, processing and managing personal data. However, the company developing the metaverse may be considered a processor if they host the diagnostic service on behalf of the doctor's practice.

What data is collected in the metaverse?

The collection and processing of personal data is inherent in the metaverse. It includes information from sensors, communications on the platform itself, payment information, identity data, location data and more. In addition to the data provided by users themselves, much data

is collected through sensors in wearable devices and the Internet of Things. This information is highly personal and includes psychological, physical, location, health and social data. According to the GDPR, this data falls under the special categories of personal data, which are subject to specific obligations.

What is the legal basis for data processing?

First, "consent" can be considered as a legal basis for data processing. However, there are some issues that may arise in the metaverse context. According to the GDPR, consent must be freely given, meaning that the data subject must not be pressured or in a relationship of authority. In situations where users are working or teaching in the metaverse, there may be an authority relationship. For example, an employee who refuses to participate in meetings in the metaverse may fear job loss, and a student who does not participate in "school outings" in the metaverse may miss important learning opportunities.

Another possible legal basis is "need to contract". The controller may process personal data if it is necessary for the performance of a contract. This may apply, for example, to the collection of biometric data via sensors to mimic a handshake. However, the processing of personal data to improve services is not allowed on this basis.

Finally, one can invoke "legitimate interest" as a legal basis for data processing. This basis requires the processor to pursue a legitimate interest that is clear, present and legitimate. The processor's interest must outweigh the rights and freedoms of the data subject. In the context of the metaverse, the economic interest may come into play, for example when using personal data for targeting. However, this legal basis must be assessed on a case-by-case basis.

Purpose limitation: avoid vagueness

The GDPR requires that personal data be collected for specific, clearly defined and legitimate purposes, and may not be further processed in a way that is incompatible with those purposes. The description of the purpose should not be too vague. For example, *"We collect personal data to improve our services"* is too vague. An improved wording would be: *"We collect data about your purchase history and use of sensors to improve the functionality of our virtual store by offering customized product recommendations."*

Special categories of personal data

Special personal data includes data on race, political opinions, religious beliefs, genetic data, biometric data and more. This data requires both a legal basis under Article 6 and justification under Article 9(2) of the GDPR.

In the metaverse, this data can be processed if the data subject has given explicit consent. However, the requirements for this consent are stricter than for ordinary consent. Instead of informed consent, it is explicit consent. This refers to how the data subject gives consent, such

as digitally signing a document.

It is also possible for aspects of life to move into this digital world. For example, tracking heart patients through sensors or tracking incapacitated individuals. In cases where the processing is necessary for preventive or occupational medicine, medical diagnosis, health care or social services, the processing of special categories of personal data is permitted.

Conclusion

The metaverse is an extension of the real world into a digital environment. By and large, the way the GDPR is applied in the real world can be applied in the metaverse. However, there are still some unique aspects of the metaverse that may present challenges for data protection authorities. The future will show how these authorities deal with them.

Silke Rogiers ***advisor legal***
s.rogiers@atern.io

Check atern.io/en/news for more finance, tax and legal news.

aternio