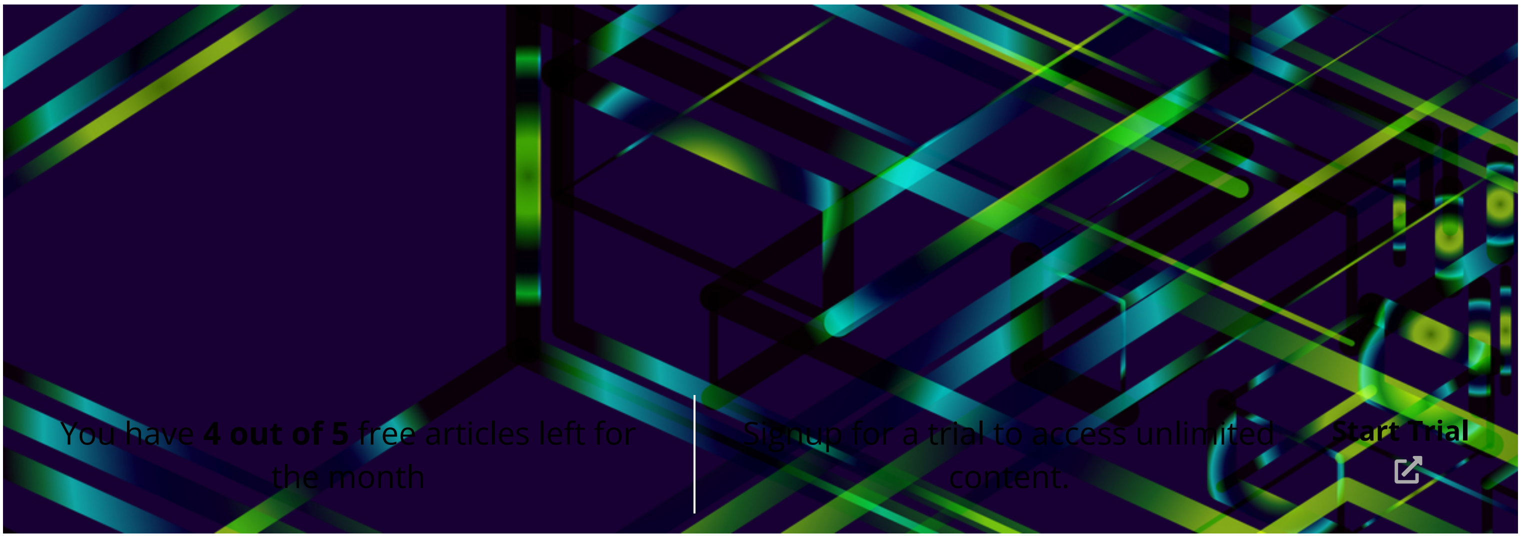
Feb 2023

International: The data vault - How to securely exchange personal data between end-users, platforms, and device manufacturers in the metaverse - Part two

Not only do interactions between end-users, platforms, and device manufacturers naturally bring along privacy concerns, but they moreover also create potential cybersecurity risks and ethical concerns. How can we ensure that end-users are properly informed, and personal data being exchanged on a legal basis in a safe and secure manner, without compromising the end-user experience?

In part two of this two-part Insight series, Danique Knibbeler, Max Mohrmann, and Sarah Zadeh, from NautaDutilh N.V., explore the possibility of a 'personal data vault', that will enable the exchange of personal data in a safe and secure manner within the metaverse, whilst also complying with data protection regulations, without compromising on interoperability and user experience. Part one focuses on the data integrity risks and ethical challenges related to the end-user and its avatar and discusses potential remedies in this regard.



shuoshu / Signature collection / istockphoto.com

Background

As touched upon in the previous Insight articles EU: Privacy and security concerns in the metaverse and part one of this two-part series, a crucial element that drives the metaverse is the requirement of seamless interoperability between third-party devices, environments, and platforms. Consequently, this interconnectedness results in a large quantity of (personal) data that is being exchanged in increasing volumes between multiple service providers in real-time.

The importance of interoperability and the risks of co-dependency

In order to provide end-users with an immersive, interoperable, and user-friendly experience between provided services and used devices, the metaverse requires high volumes of data to be exchanged quickly between the applicable services providers and device manufacturers. Due to this process, multiple 'chains' of personal data exchanges are being created, namely between end-users, device manufacturers, platform providers, and other service providers within the metaverse. However, this creates a certain 'co-dependency' between the parties involved.

If the platform and device providers in the chain do not enforce and uphold certain security standards, for example by implementing strong encryption for data transmissions and regularly updating security protocols, and a strong and privacy-compliant security framework, based on which personal data can be exchanged in a secure and transparent manner, this may lead to:

- incompatibility issues between services and/or devices that the end-user wishes to connect to; and
- security risks regarding the personal data that is being exchanged between devices and platforms.

Implementing such technical and organisational security measures to ensure a level of security appropriate to the risk is also mandatory pursuant to Article 32(1) of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). Security risks can be particularly serious in a virtual environment, such as the metaverse, where independent service providers share large amounts of personal data, special categories of personal data, such as biometric data, for identity purposes, and sensitive personal data, such as financial information for financial transactions. Therefore, only when all providers involved in the metaverse implement adequate security measures, can the end-users' experience be truly interoperable, secure, and user-friendly.

Data ownership and security risks

In the metaverse, the way personal data is exchanged across multiple platforms and between device and service providers may be untransparent to the end-user. If end-users are not informed prior to the processing of their personal data, it can be difficult for end-users to maintain control over their personal data and make informed decisions about which and how personal data is exchanged or stored. This may lead to a loss of 'data ownership'. Data ownership is based on the idea that privacy is an asset that individuals should be able to protect by exerting control over how their data is used. In practice, this means that individuals should be able to access and manage their personal data, and that organisations, such as platform providers, that collect and use personal data should do so in a responsible and ethical manner. However, the aspect of interoperability and the speed at which personal data is exchanged, as described earlier, poses a significant challenge to security. This loss of data ownership may even result in additional security issues, such as personal data breaches and unauthorised access by third parties.

The European Commission has previously stated that data ownership is a core principle for the development of new technologies. The lack of data ownership, as described above, can lead to data security breaches that have serious consequences as they thwart the reliability, availability, integrity, and confidentiality of the personal data that is being exchanged. This can result in the loss of personal data and in the worst-case scenario can be used for identity theft or other forms of fraud.

Ultimately, resolving the lack of data ownership in the metaverse will help mitigate these security risks in relation to the exchange of large amounts of personal data, whilst increasing the data ownership of the end-user, without compromising on the principles of interoperability the user-friendly security. A strong starting point could be the implementation of a decentralised data management system that preserves the interconnected nature of the metaverse when exchanging personal data.

Data management system

Ideally, a decentralised data management system enables end-users to manage and control the personal data associated with their virtual identities and assets, such as their avatars, and requires all associated providers to be transparent to the end-users about how their personal data is collected.

Although a decentralised data management system can be designed in several ways and can consist of different technical components and functionalities, we consider the main aspect to be a so-called 'data vault'. This data vault enables end-users to access their personal data via a personal account. If the end-user wishes to share personal data with platform providers, service providers, and device manufactures, the data vault gives end-users the ability to manage their privacy settings. Additional functionalities can be implemented, such as the option to give prior consent for the processing of different categories of personal data; and the option to exercise data subject rights, such as the possibility to access or modify their personal data, and to download the personal data in a structured, commonly used, and machine-readable format.

Such a system can mitigate the data ownership and security risks as mentioned above, since it provides end-users with the necessary tools to control their personal data and make informed decisions about which information to share. Nevertheless, as discussed in our previous articles, human errors are a contributing factor in over 95% of all cybersecurity incidents, and therefore, also in the metaverse, the end-user may potentially be the weakest link. Therefore, in order to safeguard the personal data, the data vault must offer a multi-layered security system and implement security measures by default, for example by:

- restricting data access when connecting to untrustworthy networks or biometric or multi-factor authentication;
- offering end-to-end encryption of the personal data with data masking features, which allows end-users to hide special categories of data, such as health data; or
- implementing logging and enabling end-users to receive notifications when their data vault is accessed by unauthorised third parties.

Conclusion

In conclusion, the data vault can create by default a stronger security and data ownership system for personal data, as it can provide a first line of defence, multiple layers of protection, transparency, control, and management capabilities for personal data, which in turn help to mitigate risks associated with data breaches and unauthorised access.

Regardless, if the concept of a data vault is executed within the metaverse, all parties involved must adhere to the minimum requirements of security surrounding personal data. Consequently, the metaverse must compromise on interoperability. Otherwise, it cannot successfully ensure a secure data management system.

However, offering this data vault will entail that not every provider can join the respective platform. Therefore, in order to still be able to guarantee the security of users' personal data, and to comply with the applicable standard in terms of technical and organisational measures that apply under Article 32(1) of the GDPR, platform providers have no choice, but to impose minimum requirements on the parties that wish to connect to the data vault and to the platform in question. However, this does mean that all parties in the chain must adhere to the same security standards so that there can be a GDPR-compliant, secure, immersive, interoperable, and user-friendly experience.

Danique Knibbeler Associate

Danique.Knibbeler@nautadutilh.com

Max Mohrmann Associate

Max.Mohrmann@nautadutilh.com

Sarah Zadeh Associate

Sarah.Zadeh@nautadutilh.com

NautaDutilh N.V., Amsterdam