

The Metaverse as a Privacy Mosaic: Framing Data Protection in Hyper-Granular, Data-Drenched Digital Ecosystems

by **Pablo Trigo Kramcsák** and **Vagelis Papakonstantinou** *

Abstract: The Metaverse unfolds as a hybrid reality, fusing physical presence with digital immersion into a sprawling ecosystem powered by continuous streams of real-time data. Behind its allure lies a sophisticated architecture, a complex web of technologies and platforms that relentlessly captures, analyses, and reshapes vast volumes of personal information. This data proliferation magnifies the stakes of privacy in ways unseen in traditional digital spaces. The Metaverse's hyper-connected nature exposes users to a novel scale of surveillance and inference, challenging established data protection norms.

This study examines these challenges in depth, moving beyond surface-level analysis to explore the intricate ecosystem of data flows that underpin virtual interactions. It proposes a tripartite taxonomy of metaverse data, distinguishing between declared, observed, and inferred data, and offering a framework to identify specific data protection risks. In examining

these dynamics, the study considers the divergent governance dynamics inherent in both centralised and decentralised metaverse architectures, recognising that these structural differences profoundly influence privacy challenges and mitigation strategies. This nuanced approach supports the development of targeted, context-sensitive strategies that embed privacy as a foundational element of the Metaverse.

Safeguarding data privacy in the Metaverse demands more than technical fixes; it calls for a fundamental rethinking of how privacy is integrated into its very architecture. This study focuses on advancing Data Protection by Design from a theoretical concept to a practical element embedded within the Metaverse Frameworks. Effective privacy protection in this setting requires a coordinated and systematic implementation of technical, organisational, and governance measures across all relevant stakeholders.

Keywords: Metaverse; virtual worlds; GDPR: data protection by design; inferred data

© 2026 Pablo Trigo Kramcsák and Vagelis Papakonstantinou

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Pablo Trigo Kramcsák and Vagelis Papakonstantinou, The Metaverse as a Privacy Mosaic: Framing Data Protection in Hyper-Granular, Data-Drenched Digital Ecosystems, 17 (2026) JIPITEC 141 para 1.

*

Pablo Trigo Kramcsák: PhD Researcher at the Law, Science, Technology and Society Research Group, Vrije Universiteit Brussel (VUB). Pleinlaan 2, Elsene, 1050, Brussel, België, Belgium. E-mail: pablo.rodrido.trigo.kramcsak@vub.be. <https://orcid.org/0000-0003-2385-4722>

Vagelis Papakonstantinou Professor of Law, Faculty of Law and Criminology, Vrije Universiteit Brussel (VUB). Pleinlaan 2, Elsene, 1050, Brussel, België, Belgium. E-mail: Vagelis.Papakonstantinou@vub.be. <https://orcid.org/0000-0002-2536-2951>

Both authors express their gratitude to the discussants and participants of the webinar “Personal Data Processing within Immersive Virtual Worlds: Compliance Challenges of the GDPR”, hosted by the Chair for the Responsible Development of the Metaverse at the University of Alicante (Spain) on 31 October 2023.

This publication was financed by the Chair for the Responsible Development of the Metaverse of the University of Alicante (Spain).

A. Introduction

- 1 The Metaverse has evolved from conceptual projections into environments where physical and digital dimensions intersect. Enabled by interconnected networks and Internet-based infrastructures, metaverse spaces operate through real-time interactions, sustained by the ongoing collection, transmission, and processing of personal data.
- 2 As immersive, metaverse-oriented applications expand and weave more deeply into social, economic, and cultural spheres, they reveal mounting tension between their underlying information streams and the constraints of traditional data protection standards. Such friction calls for a critical re-evaluation of how privacy and individual autonomy are preserved in data-intensive settings characterised by continuous processing, widespread sharing, and complex networked systems. To address this, it is necessary to identify the core privacy challenges faced by individuals interacting with these environments, while also exploring how to design metaverse ecosystems that are compliant with data protection requirements. At the same time, the conceptual fluidity of “metaverse-type” platforms complicates efforts to delineate its legal, social, and technological boundaries, underscoring the need for analytical frameworks capable of bridging existing regulatory structures with the data-driven dynamics of metaverse environments.
- 3 This paper examines the data privacy implications of immersive, metaverse-oriented applications through the lens of data protection law. Rather than framing “the Metaverse” as a *sui generis* digital realm, it situates these environments within the broader landscape of application-layer services, focusing on the taxonomies of data harvesting and the regulatory challenges they pose under existing frameworks. To develop a comprehensive understanding, Section B delineates the foundational components of the Metaverse, critically analysing its data-intensive infrastructures, enabling technologies, and immersive attributes that collectively amplify its systemic complexity.
- 4 Building upon this foundation, Section C turns to the structural distinctions between centralised and decentralised metaverse platforms. It shows how these different configurations influence core issues of data governance, user control, and the allocation of responsibilities for privacy protection. These variations are not simply architectural; they bear directly on the legal frameworks applicable to different metaverse scenarios.
- 5 Section D proceeds by classifying the types of personal data processed within metaverse

environments. The discussion ranges from basic identifiers to more complex and sensitive forms of data, including biometric information and emotional or behavioural responses. This taxonomy is essential to grasp the scope and granularity of personal data implicated in these contexts.

- 6 Section E then examines a set of personal data protection concerns that are either intensified or reconfigured by the Metaverse. It contrasts these with challenges typical of traditional online environments, highlighting how immersive features heighten existing risks.
- 7 Finally, Section F analyses the systematic integration of a Data Protection by Design (DPbD) framework within metaverse ecosystems. Such an approach, if rigorously implemented, offers a path toward embedding data protection principles directly into the architecture of these environments, rather than treating privacy as an external or secondary consideration. In doing so, the analysis also reflects on the conditions under which such integration could be meaningfully achieved.

B. The Shape of the Metaverse: Conceptual Fluidity and Technical Foundations

- 8 The word *Metaverse* resists straightforward definition,¹ having evolved into something of a conceptual wildcard in contemporary discourse. Its definitional ambiguity invites interpretation but also ensures it remains a moving target for analysis. Often described as a “catch-all” term,² the Metaverse is commonly envisioned as an immersive environment populated with 3D computer-rendered objects, spaces, and people,³ where users interact through virtual self-representations known as avatars.⁴

1 European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs, ‘Metaverse - Study requested by the JURI Committee’ (2023), 10 [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU\(2023\)751222_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf) accessed 10 July 2025.

2 Luciano Floridi, ‘Metaverse: a Matter of Experience’ (2022) 35 *Philosophy and Technology* 1, 73.

3 Mariana Olaizola Rosenblat, ‘Reality Check: How to Protect Human Rights in the 3D Immersive Web’ (2023) NYU Stern Center for Business and Human Rights, September 2023, 1 <https://bhr.stern.nyu.edu/publication/reality-check-how-to-protect-human-rights-in-the-3d-immersive-web/> accessed 10 July 2025.

4 Ben Chester Cheong, ‘Avatars in the metaverse: potential legal issues and remedies’ (2022) *Int. Cybersecur. Law Rev* 3, 467–494, 472.

- 9 Despite this openness, several recurring features help to sketch its contouring architecture. Virtual worlds are generally understood to possess three fundamental characteristics: persistence and real-time functionality, immersive user experiences, and integrated economic and social interaction mechanisms.⁵ Supporting these features requires four core technical attributes: Realism, fostering emotional immersion and a sense of presence; Ubiquity, ensuring consistent access and identity across devices; Interoperability, allowing seamless interaction across platforms; and Scalability, enabling the system to accommodate growing user demand without compromising performance.⁶ From a data governance perspective, these characteristics are significant because they shape and intensify the collection, processing, and inference of personal and non-personal data across multiple technological modalities.
- 10 Although often presented as a rapidly shifting frontier, the Metaverse has so far experienced measured—rather than transformative—advances in autonomy, capacity, and functionality. Developments in the Internet of Things (IoT), virtual reality (VR), augmented reality (AR), mixed reality (MR), and extended reality (XR),⁷ alongside improvements in internet infrastructure and device performance, have contributed to the creation of more immersive digital spaces.⁸ Virtual environments increasingly feature broader application scopes, improved cross-technology compatibility, and smoother integration with smart devices, giving rise to more convincing and interactive experiences.
- 11 Public and private entities are exploring ways to leverage metaverse environments, integrating them into their processes, services, and business models,⁹ thereby impacting a variety of activities and industries.¹⁰ Central to this development are the social and economic interactions that drive these virtual worlds.¹¹ As a result, there is increasing attention and debate about the potential socio-economic implications of the Metaverse on a global scale.¹²
- 12 The term Metaverse can be used both in the singular and the plural. As a singular concept, it represents a unified and interconnected digital universe, that encompasses multiple platforms and environments, similar to the internet or cyberspace. In contrast, using “Metaverses” in the plural acknowledges the current reality of multiple distinct virtual worlds, each with its own architecture, governance, and user base. This plural form, which has drawn most scholarly attention over recent decades,¹³ reflects the fragmentation and diversity of virtual spaces (as “micro-universes”) shaped by varying providers, technologies, and regulatory frameworks. The singular emphasises the aspirational and integrated vision of a comprehensive digital environment, while the plural highlights the practical multiplicity and heterogeneity of existing immersive ecosystems.¹⁴
- 13 This study takes a functional and conceptual view of the Metaverse as a new data-driven stage of the Web, emphasising the interactions, data flows, and governance arrangements that link its diverse
-
- 5 European Commission and the Multi Stakeholder Platform on ICT Standardisation (MSP), ‘Rolling Plan for ICT Standardisation - Metaverse’ (2023) <<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/metaverse#>> accessed 10 July 2025.
- 6 European Parliamentary Research Service (EPRS), ‘Metaverse: Opportunities, Risks and Policy Implications’ (2022) <https://www.europarl.europa.eu/cmsdata/268589/eprs-briefing-metaverse_EN.pdf> accessed 10 July 2025.
- 7 Agencia Española de Protección de Datos, ‘Metaverse and Privacy’ (www.aepd.es, 29 September 2022) <<https://www.aepd.es/en/prensa-y-comunicacion/blog/metaverse-and-privacy>> accessed 10 July 2025. VR, AR, MR, and XR are key concepts in the evolving landscape of immersive technologies. VR provides a fully immersive experience within a computer-generated environment, while AR enhances the real world by overlaying it with digital content. MR takes AR a step further by enabling users to interact with and manipulate digital objects within their physical surroundings. XR serves as an umbrella term that encompasses all these forms of computer-altered realities (Olaizola Rosenblat (n 3) 4).
- 8 Arjun Nagendran and others, ‘Avatar Led Interventions in the Metaverse Reveal That Interpersonal Effectiveness Can Be Measured, Predicted, and Improved’ (2022) 12 *Scientific Reports* 1, 21892.
-
- 9 Yogesh K Dwivedi and others, ‘Metaverse beyond the Hype: Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy’ (2022) 66 *International Journal of Information Management* 102542, 2.
- 10 Lau Christensen and Alex Robinson, ‘The Potential Global Economic Impact of the Metaverse’ (2022) Analysis Group, 2 <https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse.pdf> accessed 10 July 2025.
- 11 Mitchell Goldberg and Fabian Schär, ‘Metaverse Governance: An Empirical Analysis of Voting within Decentralized Autonomous Organizations’ (2023) 160 *Journal of Business Research* 113764.
- 12 See, e.g., World Economic Forum, ‘Social Implications of the Metaverse’ (2023) https://www3.weforum.org/docs/WEF_Social_Implications_of_the_Metaverse%20_2023.pdf accessed 10 July 2025.
- 13 Lorena Arismendy Mengual, ‘Liability for Wrongful Behaviour in the Metaverse’ (2024) 15(3) *JIPITEC* 229, 230.
- 14 “[I]t may be more appropriate to refer to metaverses in the plural, assuming that there will not be a single metaverse platform.” (Dwivedi et al. (n 9) 25).

applications and platforms. It encompasses a wide array of applications, platforms, services, and data-intensive technologies—both centralised and distributed—that operate atop digital infrastructures, rather than constituting isolated enclaves. These applications engage with users and one another, while operators and service providers intervene in governance, management, and data-handling processes. The analysis focuses on the shared logics of data processing across these environments, while recognising technological distinctions where they are relevant for data privacy implications.

- 14 To understand these shared logics in practice, it is necessary to examine the flows of information that traverse both immersive and physical environments, and the infrastructures that enable such continuous data processing.
- 15 The Metaverse integrates inputs from the physical world with data generated within virtual environments, creating a multifaceted informational landscape. This data varies in nature. Some remain static, while others, such as location and sensor readings, are dynamic and continuously evolving.¹⁵ Supporting this complexity is an equally sophisticated infrastructure composed of interconnected sensors, actuators, and networks. Sensors capture real-time information from the environment, while actuators convert digital commands into physical responses.¹⁶ Together, these components establish a bidirectional interface that facilitates interaction between physical and virtual realms, a prerequisite for Metaverse functionality.¹⁷

C. Who Holds the Keys? Typing the Metaverse(s) Through Governance and Structure

- 16 Digital environments commonly described as metaverse applications are not merely technical infrastructures; they function as social and economic systems that reflect and shape the rules governing participant interaction. Governance arrangements (including the allocation of power, the structuring of authority, and the distribution of control over

resources) not only influence how users engage with these environments but also have significant implications for privacy, data protection, security, and individual agency.

- 17 Platforms occupy a central role in structuring the Metaverse, shaping how people move, interact, and make sense of these digital spaces. They set the rules of participation, decide who can access what, and guide how information is collected, used, and shared. Within the Metaverse, these platforms can be broadly distinguished according to their governance and technical structures as centralised or decentralised.¹⁸ These models do more than define technical and operational structures; they fundamentally shape the governance frameworks that regulate power, control, and decision-making within these virtual environments. Centralised metaverse platforms, typically large-scale virtual environments, concentrate governance in a single entity or a small group of actors, establishing clear hierarchies and tightly controlled spaces in which authority, decision-making, and resource allocation reside with a limited few. In contrast, decentralised settings aim for a more distributed form of governance, granting users greater autonomy and influence over their virtual interactions. However, the distinction is not always absolute. Some platforms integrate elements from both models, resulting in hybrid systems.¹⁹
- 18 A centralised environment resembles traditional internet platforms, where a few entities have significant power over the infrastructure, governance, and data. Such configurations rely on central servers managed by a single entity.²⁰ A central authority oversees the entire ecosystem, determining and enforcing rules, policies, and governance, while users wield limited influence over decision-making processes. This central stakeholder often exerts substantial control over user data, encompassing its collection, copy, storage, and dissemination (for example, managing user identities, authentication, and profiles).
- 19 Decentralised platforms, by contrast, operate on distributed architectures, where governance, technical infrastructure, and key components are spread and shared across multiple nodes or participants.²¹ In principle, this model allows for

15 Beng Chin Ooi and others, 'The Metaverse Data Deluge: What Can We Do About It?' in *IEEE 39th International Conference on Data Engineering (ICDE)* (Institute of Electrical and Electronics Engineers (IEEE), 2023), 3675-3687, 3678.

16 Xinyi Tu and others, 'Architecture for data-centric and semantic-enhanced industrial metaverse: Bridging physical factories and virtual landscape' (2024) *Journal of Manufacturing Systems* 74, 965-979, 968.

17 Tero Kaarlela and others, 'Towards Metaverse: Utilizing Extended Reality and Digital Twins to Control Robotic Systems' (2023) 12 *Actuators* 6, 219.

18 Liang Yang and others, 'Interoperability of the Metaverse: A Digital Ecosystem Perspective Review' (SSRN, 13 June 2024) <https://ssrn.com/abstract=4929167> accessed 12 July 2025, 9.

19 Ikram Ud Din and others, 'Integration of IoT and Blockchain for Decentralized Management and Ownership in the Metaverse' (2023) 36 *International Journal of Communication Systems* e5612.

20 Yang et al. (n 18).

21 Omar Hashash and others, 'Towards a Decentralized Metaverse: Synchronized Orchestration of Digital Twins

greater user autonomy and ownership, as well as peer-to-peer interactions. This has significant implications in how digital assets are managed, how content moderation is approached, and how compatibility across different clients and devices is supported,²² potentially enabling more flexible metaverse environments. It often uses blockchain technology and distributed protocols to support its features, which impacts the levels of decentralisation.²³ While stakeholders and users may engage actively in the governance and development of this model, they inevitably face the significant technical complexities and coordination challenges embedded within its inherently distributed structure.

- 20 Hybrid platforms combine elements of both models, integrating centralised oversight with decentralised participation or technical features. These systems illustrate the spectrum of governance approaches within the Metaverse, highlighting the trade-offs between control, user agency, and technical complexity.

D. Dissecting Metaverse Personal Data Processing: A Taxonomy of What Is Collected, Generated, and Analysed

- 21 Viewed through the lens of its core characteristics and technical foundations, the Metaverse is made up of interconnected applications and services that work together to create continuity, responsiveness, and a palpable sense of presence. Its persistence, real-time functionality, and immersive nature are not incidental features: they depend on the constant generation and processing of user data. Rather than remaining passive spectators, users serve as continuous sources of input in the creation of metaverse objects,²⁴ feeding ubiquitous and realistic environments engineered to track, analyse, and adapt to their every action. This dynamic is sustained through multi-sensor fusion,²⁵ whereby streams of data such as gaze direction, voice, motion, and biometric signals are continuously captured and processed. These inputs enable the system

to respond in real time and tailor interactions to individual users, reinforcing the sense of immersion.

- 22 The sheer complexity and interdependence of these data flows resist simplification into mere categories. Beyond the traditional distinction between special and non-special categories of personal data, often framed as sensitive and non-sensitive, a nuanced taxonomy is necessary to differentiate data according to its origins, modes of collection, and methods of production. Such a taxonomy is crucial, as it exposes the varying degrees of control, responsibility, and legal significance inherent in each type, thereby laying the groundwork for meaningful governance and accountability.
- 23 Broadly speaking, personal data processed within metaverse applications can be classified into three principal categories: declared data, which users voluntarily provide;²⁶ observed data, which emerges from their behaviours, interactions, and preferences;²⁷ and inferred data, which is generated through the analysis and correlation of existing information.²⁸ This tripartite taxonomy thus aligns closely with the technical architectures and operational realities in the Metaverse, encompassing all data generated and used in it. Together, these categories correspond to distinct stages of data flow, beginning with user engagement and sensing and progressing to complex computation, thereby offering a comprehensive framework for understanding how information is created,

and Sub-Metaverses' in *Proceedings of the IEEE International Conference on Communications (ICC '23)* (Institute of Electrical and Electronics Engineers (IEEE), 2023), 1905-1910, 1905.

22 Goldberg and Schär (n 11).

23 Nir Kshetri, 'A Typology of Metaverses' (2022) 55 *Computer* 12, 150-155.

24 Thien Huynh-The and others, 'Blockchain for the metaverse: A Review' (2023) *Future Generation Computer Systems* 143, 401-419, 406.

25 Ruoyu Zhao and others, 'Metaverse: Security and Privacy Concerns' (2023) 3 *Journal of Metaverse* 2, 93-99.

26 It has been defined in the literature as 'data actively and knowingly provided by the data subject' (Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability – WP 242 rev.01, 5 April 2017' (2017) 10 <https://ec.europa.eu/newsroom/article29/items/611233> accessed 10 July 2025).

27 A useful way to describe it is as 'data provided by the data subject by virtue of the use of the service or the device' (Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability – WP 242 rev.01, 5 April 2017' (2017) 10 <https://ec.europa.eu/newsroom/article29/items/611233> accessed 10 July 2025).

28 Inferred data (or derived data) 'refers to data which is created by the controller on the basis of the data provided by the data subject (regardless of whether these data were observed or actively provided by the data subject, or a combination thereof)' (European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users. Version 2.0. Adopted on 13 April 2021' (2021) https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf accessed 10 July 2025, 24.).

transformed, and mobilised within the metaverse systems.

I. Declared Data

- 24 This data represents information users willingly and consciously share while interacting in virtual worlds. The significance of declared data lies in its direct and explicit nature. At a general level, this category encompasses:
- 25 (1) User profiles and personal details. User profiles are a key component of declared data, allowing individuals to create and manage their digital identity. These profiles typically include basic information such as name, age, and gender, alongside demographic data, preferences, social connections, and virtual achievements.²⁹ Notably, this data underpins the creation and ongoing customisation of avatars, which act as the user's digital embodiment. Serving as the primary interface for interaction and communication, avatars anchor the user's presence and facilitate meaningful engagement within the Metaverse.³⁰ Declared data shapes avatars' appearance, behaviour, and backstory, reflecting users' desired identity and roles within virtual settings. It forms a curated digital self, crafted through personal choices in metaverse social contexts.
- 26 (2) Preferences. During account setup or at any point thereafter, users can select their interests, hobbies, and specific preferences, allowing for a more personalised virtual experience. These preferences can range from choosing themes for content to specifying the type of interactions they wish to have, reflecting their personal inclinations and goals within the virtual world.

II. Observed Data

- 27 This category encompasses data generated through users' actions, interactions, and behaviours. The Metaverse's technological features extend the capacity not only to collect but also to observe and record detailed information from both physical and virtual worlds, often integrating inputs from service providers or third parties, thereby broadening the scope of data capture. Metaverse devices and sensors often draw on information from the physical world to

enhance immersion,³¹ relying on inputs from service providers or third parties. The underlying goal is to synchronise input and output modalities, fostering a more seamless and integrated experience.³² Observed data may include a broad spectrum of elements, such as:

- 28 (1) User activities. This encompasses data generated through users' movements, interactions with virtual objects, and in-world behaviours. Its implications extend beyond active participants, potentially impacting individuals not directly engaged in the Metaverse. For example, VR headsets equipped with external cameras and motion sensors may capture data from users' physical surroundings,³³ including bystanders who fall within the device's tracking range.³⁴ Such incidental data collection can erode anonymity, exposing individuals to forms of digital fingerprinting.³⁵
- 29 (2) Sensorial data. Derived from users' embodied interactions and perceptual engagement, this data includes visual inputs obtained through micro-optics and image recognition systems, auditory information such as voice and ambient soundscapes, and tactile feedback mediated by haptic gloves, bodysuits, touchscreens, or biometric sensors. More broadly, it draws on corporeal cues (eye movements, facial micro-expressions, postural shifts, and gestural patterns)³⁶ that serve as proxies for affective or cognitive states. For instance, iris dynamics captured by VR headsets or posture variations detected by motion controllers may provide insights into a user's emotional or attentional orientation.³⁷
- 30 (3) Communication logs. Capturing the full spectrum of interaction, these logs record both the content and metadata of user exchanges, including voice chats, written messages, gestures, and symbolic

29 See Daniel Zimmermann, Anna Wehler and Kai Kaspar, 'Self-representation through avatars in digital environments' (2023) 42 *Current Psychology* 21775.

30 Martin Ebers, 'Avatars and the Protection of Digital Identities in the Metaverse' (MetaverseUA Research Paper No 3, 2024) 4 <https://metaversechair.ua.es/working-papers/> accessed 12 July 2025.

31 Lik-Hang Lee and others, 'All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda' (2021) 14 *Journal of Latex Class Files* 8, 41.

32 Ibid.

33 Bristows, 'Data protection in the metaverse' (www.bristows.com, 27 October 2022) <https://www.bristows.com/news/data-protection-in-the-metaverse/> accessed 13 July 2025.

34 Vasilis Xynogalas and Mark Leiser, 'The Metaverse: searching for compliance with the General Data Protection Regulation' (2024) 14 *International Data Privacy Law* 2, 89-105, 100.

35 Daniel Berrick and Jameson Spivack, 'Understanding Extended Reality Technology & Data Flows' (Future of Privacy Forum Blog, 17 November 2022) <https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/> accessed 13 July 2025.

36 Olaizola Rosenblat (n 3).

37 Agencia Española de Protección de Datos (n 7).

communication alike. More than simple records, they could serve as a dynamic archive, enabling fine-grained analysis of social dynamics, linguistic patterns, and relational flows.

- 31 (4) Location tracking. The Metaverse relies on geospatial technologies to fuse physical and virtual spaces, supporting location-based services and digitally grounded experiences through precise spatial data.³⁸ In this context, location data entails more than simple coordinates. It captures users' movements, choices of virtual locations, and temporal patterns across virtual environments. This continuous mapping reveals habits of presence and affinities for specific areas, providing input for behavioural analytics.
- 32 (5) Virtual transactions. Each in-game purchase, currency exchange, or asset transfer produces economic metadata that extends beyond the transaction itself. For instance, in decentralised virtual environments, inventory management systems can monitor the movement and ownership of digital assets over time.³⁹ These transactional records form detailed consumption profiles, revealing not only what users acquire but also the timing, methods, and contextual factors influencing their decisions.

III. Inferred Data

- 33 This category consists of information not directly disclosed or recorded but rather generated through analytical processes applied to human traits and behaviours by third-party actors.⁴⁰ It involves interpreting patterns drawn from existing data, turning raw inputs into new insights. As a derivative form of data,⁴¹ it reflects knowledge produced from both declared and observed information, often through advanced analytical techniques, including AI-driven decision-making systems.⁴² For example,

motion-based fingerprinting can reveal specific traits about a user, and when combined with other tracked data, it can significantly enhance identification accuracy.⁴³ Similarly, a wide range of personal information can be inferred simply by analysing motion data captured by VR devices,⁴⁴ potentially exposing sensitive aspects of an individual's life, including medical conditions, physical impairments, or past traumas.⁴⁵

- 34 Inferred data quietly shapes the architecture of the Metaverse, drawing on users' expressed preferences and behavioural patterns to generate detailed profiles. These profiles drive personalised features such as content suggestions, virtual interactions, and purchase recommendations. Advertisers rely on this data to align messages with users' likely interests, increasing engagement while raising concerns about manipulation and profiling. At the same time, inferred data supports the automation of tasks and the anticipation of user needs.

E. Fractured Privacy: Mapping Personal Data Risks in the Metaverse

- 35 As detailed in previous sections, the Metaverse is built upon a distinctly data-centric foundation that reshapes the generation, collection, and use of information. This systemic reconfiguration underscores a fundamental departure from traditional digital environments, leading to privacy challenges that go beyond traditional concerns.
- 36 Powered by technologies enabling multisensory interactions,⁴⁶ such as wearable haptic devices and

38 Theofilos Papadopoulos and others, 'The Metaverse Is Geospatial: A System Model Architecture Integrating Spatial Computing, Digital Twins, and Virtual Worlds' (2025) 14 *ISPRS International Journal of Geo-Information* 126, 7.

39 Durgesh Pandey and Paul Gilmour, 'Accounting Meets Metaverse: Navigating the Intersection Between the Real and Virtual Worlds' (2024) 22(2) *Journal of Financial Reporting and Accounting* 211, 221.

40 Luca Bolognini and Marco Emanuele Carpenelli, 'The future of personal data in the Metaverse' (2022) Istituto Italiano per la Privacy e la Valorizzazione dei Dati <https://zenodo.org/records/6413046> accessed 13 July 2025, 8.

41 Mark Elliot and others, 'Inferred Data' in Mark Elliot, Anna M Mandalari, Miranda Mourby and Kieron O'Hara (eds), *Dictionary of Privacy, Data Protection and Information Security* (Edward Elgar Publishing, 2024).

42 AI tools could be relevant, among other aspects, for the

operation of automatic digital twins, computer agents and the autonomy of the avatar (Lee et al. (n 31)).

43 Louis Rosenberg, 'Privacy in the Metaverse might be Impossible (new research study)' ([www.medium.com](https://medium.com/predict/privacy-in-the-metaverse-might-be-impossible-new-research-study-64935481c6de), 30 March 2023) <https://medium.com/predict/privacy-in-the-metaverse-might-be-impossible-new-research-study-64935481c6de> accessed 14 July 2025.

44 Vivek Nair and others, 'Inferring Private Personal Attributes of Virtual Reality Users from Head and Hand Motion Data' (2023) arXiv <https://arxiv.org/abs/2305.19198> accessed 14 July 2025.

45 Eleonora Margherita Auletta, Francesca Tugnoli and Giada Iovane, 'Personal data protection in the Metaverse: operational challenges and regulatory uncertainties' (www.ictlc.com, 28 September 2022) https://www.ictlc.com/personal-data-protection-in-the-metaverse-operation-challenges-and-regulatory-uncertainties/?lang=en#_ftn4 accessed 14 July 2025.

46 Stylianos Mystakidis, 'Metaverse' (2022) 2 *Encyclopedia* 1, 486-497, 487.

the Internet of Things,⁴⁷ The Metaverse captures a vast spectrum of personal data, gathering far more sensitive information than conventional platforms.⁴⁸ Internet-connected wearables continuously monitor users, collecting diverse data types, including physical metrics, user habits and preferences, and communication patterns.⁴⁹ Auxiliary devices designed for metaverse applications go further, capturing increasingly intrusive biometric information.⁵⁰ The volume and granularity of information XR technologies collect far exceed that of traditional surveillance tools, making them markedly more invasive.⁵¹ Beyond raw data, virtual spaces rely on advanced analytics,⁵² allowing it to draw extensive inferences that deepen the scope and sensitivity of knowledge about users.

- 37 Metaverse's data practices extend their reach beyond corporeal data, raising profound implications for mental autonomy,⁵³ by progressively penetrating users' cognitive and emotional spheres. While earlier devices were largely limited to tracking basic physiological functions, today's tools map psychological processes, preferences, and emotional states.⁵⁴ When deployed together, these systems generate compound effects, both individual and societal, that raise serious and unpredictable risks to rights and freedoms.⁵⁵

- 38 In parallel, stakeholders in the metaverse ecosystem actively monetise and trade the data they collect,⁵⁶ embracing extraction-driven business models that prioritise continuous tracking and behavioural profiling. This data possesses substantial economic value, both as a standalone commodity and as a resource that can be repurposed, aggregated, and sold across various markets and sectors,⁵⁷ including advertising, insurance, and predictive analytics.

- 39 Metaverse technologies, however, do not create uniform challenges, as each generates data in ways that are technically and legally distinct. VR applications capture highly detailed behavioural and spatial information, AR systems integrate environmental and sensor data, and IoT/XR platforms continuously stream telemetry from connected devices. The intensity, granularity, and type of data thus vary across systems, stretching traditional privacy safeguards to their limits. While existing regulatory frameworks already cover these activities, the sprawling and interconnected nature of metaverse systems' data flows places established protections, particularly the European Union's General Data Protection Regulation (GDPR),⁵⁸ under significant pressure.⁵⁹ The GDPR's broad material scope covers a wide range of personal data processing,⁶⁰ making models that facilitate immersive user interactions clearly subject to its regulatory framework.⁶¹

- 40 For instance, Metaverse's extensive and granular data collection dynamics strain the principles of

47 Kisoo Kim and others, 'Metaverse Wearables for Immersive Digital Healthcare: A Review' (2023) 10 *Advanced Science* 4.

48 Dwivedi et al. (n 9) 8.

49 Lee et al. (n 31) 39.

50 Kewa Jiang, 'Protecting Mental Health Data Privacy in the Metaverse: How Does That Make You Feel?' (2023) 28:1 *Intell Prop & Tech LJ* 23, 28.

51 Olaizola Rosenblat (n 3) 9.

52 Leon Anidjar and others, 'The Matrix of Privacy: Data Infrastructure in the AI-Powered Metaverse' (February 18, 2023). Harvard Law & Policy Review, Forthcoming <https://ssrn.com/abstract=4363208>. It should be noted that convergence of AI and XR is transforming immersive technologies, making AI essential in prediction, personalisation, interaction, speech recognition, and language translation. This evolution raises the question of whether the combination of generative AI and XR will become the next major platform (Susan Ariel Aaronson and Adam Zable, 'Facing Reality: Canada Needs to Think about Extended Reality and AI', CIGI Papers No. 289 — March 2024 (2024) <https://www.cigionline.org/static/documents/no.289.pdf> accessed 14 July 2025, 6).

53 Council of Europe and IEEE Standards Association, 'The Metaverse and Its Impact on Human Rights, the Rule of Law and Democracy' (2024) <https://rm.coe.int/the-metaverse-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce> accessed 14 July 2025, 7.

54 Marcello Ienca and Gianclaudio Malgieri, 'Mental data protection and the GDPR' (2022) 9 *Journal of Law and the Biosciences* 1, 2.

55 Agencia Española de Protección de Datos (n 7).

56 Zefeng Chen and others, 'Metaverse Security and Privacy: An Overview' in 2022 *IEEE International Conference on Big Data (Big Data) Dec. 17 2022 to Dec. 20 2022 Osaka, Japan* (Institute of Electrical and Electronics Engineers (IEEE), 2022), 2950-2959.

57 See Ben Egliston and Marcus Carter, 'Critical questions for Facebook's virtual reality: data, power and the metaverse' (2021) 10 *Internet Policy Review* 4.

58 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 (4 May 2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

59 Maryant Fernández, 'Call for Evidence on an EU Initiative on Virtual Worlds - BEUC's Response' (www.beuc.eu) <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-053_Call_for_evidence_on_an_EU_initiative_on_virtual_worlds.pdf> accessed 16 July 2025.

60 See Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40.

61 Baily Martin, 'Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse' (2022) 36(1) *Harvard Journal of Law & Technology* 235, 256.

purpose limitation and data minimisation, which are designed to restrict the scope and necessity of personal data processing. These principles presume a degree of control and predictability that is often absent in immersive environments, where data is collected continuously, contextually, and often passively. Additionally, the Metaverse relies on layered technical infrastructures, intersecting systems, and a strong push for interoperability, making the consistent application of privacy protections across actors and platforms particularly difficult. As a result, translating the GDPR's normative commitments into operational safeguards in these environments becomes a deeply complex undertaking.

- 41 This scenario makes it increasingly necessary to move beyond surface-level assessments and confront the specific regulatory challenges the Metaverse poses. At stake is not merely compliance, but the viability of applying core privacy principles in an environment where data is ambient, inferential, and persistently in motion.

I. Intensive Data Collection and Detailed Profiling

- 42 Virtual environments' architecture fosters a level of monitoring that exceeds traditional applications,⁶² allowing for the fusion of heterogeneous sources,⁶³ and the continuous tracking of user behaviour with heightened precision.
- 43 This situation not only gives rise to new privacy concerns but also amplifies existing ones,⁶⁴ elevating 'the risk of invasion of privacy'.⁶⁵ To illustrate, these spaces could monitor the user's features such as facial expressions, voice inflections, postures and, if allowed, vital signs, including heart rate, blood pressure, respiration rate, pupil dilation, and even galvanic skin response.⁶⁶ In addition, the immersive aspect of the Metaverse could reduce the users' ability and perception to make decisions that
- prevent the excessive collection and processing of personal data.⁶⁷
- 44 All of this highlights the implications of the Metaverse's data logic, which is rooted in the sheer complexity and heterogeneity of data sources it activates. The Metaverse mirrors and duplicates lived reality,⁶⁸ generating data not only from deliberate user actions but also from ambient, often passive, sensory inputs.⁶⁹ These inputs, whether behavioural, physiological, or environmental, are persistently recorded, producing a flow of information that is continuous and profoundly difficult to contain.
- 45 Within sensor-rich, behaviour-driven immersive environments, the capacity to derive inferences extends far beyond personalisation or optimisation. It reshapes how knowledge about individuals is generated and applied, enabling datafication to penetrate deeply into personal identity and decision-making processes. The outcome is the construction of granular, multilayered profiles that surpass the analytical capacities of earlier digital environments.⁷⁰
- 46 These enhanced profiles create fertile ground for highly targeted and, at times, intrusive marketing practices, including avatar-based promotions.⁷¹ Advertisers can also measure the effectiveness of their campaigns more precisely by leveraging data collected through XR technologies, including eye movements, pupil dilation, and heartbeat.⁷² These practices contribute to ongoing surveillance and invade individuals' intimate virtual spaces, undermining their autonomy over digital experiences. The concern lies not merely in the accuracy of these inferences and profiles but in their opaque capacity to shape perceptions, interactions,
-
- 62 European Data Protection Supervisor, 'Metaverse' (www.edps.europa.eu) <https://edps.europa.eu/press-publications/publications/techsonar/metaverse> accessed 16 July 2025.
- 63 Ooi et al. (n 15).
- 64 Martin (n 61) 254.
- 65 Hang Wang and others, 'A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges' (2023) 10 *IEEE Internet of Things Journal* 16, 14671–14688, 14672.
- 66 Louis Rosenberg, 'The Growing Need for Metaverse Regulation', in Kohei Arai (ed) *Intelligent Systems and Applications. IntelliSys 2022. Lecture Notes in Networks and Systems*, vol 544 (Springer, Cham, 2023), 544.
- 67 Philipp Koehler, 'The Metaverse and some of its emerging challenges for data protection law' (www.taylorwessing.com, 10 October 2022) <https://www.taylorwessing.com/en/insights-and-events/insights/2022/10/the-metaverse-and-some-of-its-emerging-challenges-for-data-protection-law> accessed 16 July 2025.
- 68 Janna Anderson and Lee Rainie, 'The Metaverse in 2040' (www.pewresearch.org, 30 June 2022) <https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/> accessed 16 July 2025.
- 69 Mystakidis (n 46) 488.
- 70 Agencia Española de Protección de Datos (n 7).
- 71 See, for example, Kyle Coble, Jay Ratican and James Hutson, 'Beyond the pixelated mirror: Understanding avatar identity and its impact on in-game advertising and consumer behavior' (2023) 4 *Metaverse* 2023 2, 2377.
- 72 Bristows (n 33).

and decisions, often without meaningful transparency or accountability.

II. Identity, Authentication and Anonymity

- 47 In virtual spaces, the varied identity requirements across platforms give rise to substantial vulnerabilities for users. These vulnerabilities include threats ranging from identity theft to online harassment.⁷³ It is particularly important to recognise the extent to which biomechanics may serve as unique identifiers in virtual reality.⁷⁴ As users engage with virtual environments, their movements, speech patterns, and other behaviours generate data that may fully reveal their identities.⁷⁵
- 48 Compounding these risks, avatars often fail to adequately shield users' true identities. They may be linked to personal information or accounts accessible to metaverse service providers and shared with other stakeholders. Even minimal data, such as the basic motion tracking used for interaction in virtual worlds, can uniquely identify individuals, undermining meaningful anonymity.⁷⁶ Researchers refer to this as "telemetry data," the minimal dataset needed for natural user interaction,⁷⁷ which nevertheless holds outsized power for profiling. Recent studies underscore just how easily VR users can be profiled and deanonymised.⁷⁸

73 Anna Maria Collard, 'Crime in the metaverse is very real. But how do we police a world with no borders or bodies?' (www.weforum.org, 18 August 2022) <https://www.weforum.org/agenda/2022/08/crime-punishment-metaverse/> accessed 10 February 2024.

74 Vivek Nair and others, 'Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data' in *32nd USENIX Security Symposium (USENIX Security 23)* (USENIX Association, 2023), 895-910.

75 World Economic Forum, *Metaverse Identity: Defining the Self in a Blended Reality – Insight Report March 2024* (2024) https://www3.weforum.org/docs/WEF_Metaverse_Identity_Defining_the_Self_in_a_Blended_Reality_2024.pdf accessed 16 July 2025.

76 See Ronald Leenes, 'Privacy in the Metaverse' (2008), in Simone Fischer-Hübner and others (eds) *The Future of Identity in the Information Society. Privacy and Identity 2007. IFIP – The International Federation for Information Processing*, vol 262 (Springer, Boston, MA, 2008).

77 Rosenberg (n 66).

78 Vivek Nair, Gonzalo Munilla-Garrido and Dawn Song, 'Going Incognito in the Metaverse: Achieving Theoretically Optimal Privacy-Usability Tradeoffs in VR' in *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology (UIST '23)* (Association for Computing Machinery, New York, 2023) Article 61, 1-16.

- 49 The regulatory scope is not confined to explicit data disclosures. While avatars are often designed to support pseudo-anonymity, they can nevertheless expose users' real-world identities through inference. The physical and demographic attributes assigned to an avatar, such as body shape, skin tone or clothing, may closely mirror or idealise aspects of the user's authentic self,⁷⁹ creating a connection that undermines anonymity. In some instances, these representations may engage special categories of personal data under Article 9 GDPR, particularly when avatars realistically reflect sensitive characteristics.⁸⁰ Assumptions or inferences drawn from avatar features, especially when combined with other data or assessed in the context of specific processing activities, may also qualify as special category data.⁸¹ This includes politically sensitive attributes, sexual orientation and other protected aspects of identity that may be revealed through virtual representation and behavioural patterns.⁸²

III. Data Subjects' Consent, Transparency and Control

- 50 In metaverse environments, many platforms and stakeholders acting as data controllers often fall short of providing clear and accessible information regarding the use of personal data.⁸³ Likewise, users are not always offered straightforward mechanisms to manage data-sharing preferences or to track how their information is processed over time. As a result, individuals may lack the necessary insight to make informed, specific, and voluntary decisions about their data.⁸⁴ This, in turn, diminishes the practical effectiveness of consent as a legal basis for processing, particularly when users do not fully understand the scope, purposes, or potential consequences of the data practices they are subjected to.
- 51 In this context, multiple data controllers frequently operate simultaneously, processing high volumes of personal data in real time. The pace and scope of data collection complicate efforts to maintain transparency, further blurring the boundaries of

79 Zimmermann et al. (n 29).

80 Bristows (n 33).

81 European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users. Version 2.0. Adopted on 13 April 2021' (2021) https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf accessed 10 July 2025, 30.

82 European Data Protection Supervisor (n 62).

83 Xynogalas and Leiser (n 34) 99.

84 See, for example, Jasmine Wang and Eddie Liu, 'Data Usage in Social Media' (www.medium.com, 24 December 2020) <https://medium.com/big-data-at-berkeley/data-usage-in-social-media-21d606ec4451> accessed 17 July 2025.

consent.⁸⁵ Metaverse contexts also merge different purposes for processing, making it difficult for the data subjects to consent for each purpose separately.⁸⁶ Providing users with adequate information about what data is processed, how it is used, and for what purposes becomes not only burdensome but structurally difficult. This undermines compliance with the principles of purpose limitation, fairness, and transparency.⁸⁷

52 Two models for operationalising consent in the Metaverse emerge. One adopts a unified consent framework applicable across the entire environment. The other allows each entity to establish and govern its own rules.⁸⁸ The effectiveness of either approach hinges on the distribution of power between users and platform stakeholders.⁸⁹ Where dominant actors exert control over infrastructure, services, or devices, users' ability to meaningfully consent is significantly weakened. This asymmetry raises concerns regarding the processing of special categories of personal data under Article 9(2) GDPR, which requires explicit consent in the form of an express, unambiguous statement.⁹⁰

53 Consent becomes even more fraught when children are involved. Under the GDPR, valid consent requires that the child has sufficient capacity to grasp the implications of the data processing activity. Where such capacity is lacking, consent cannot be considered informed, and the data controller must instead seek authorisation from a parent or legal guardian.⁹¹

85 Moerel points out that '[p]rivacy and data security issues will be exacerbated in the metaverse and obtaining any form of meaningful informed consent will prove a practical impossibility' (Lokke Moerel, 'Metaverse and data protection', in Larry A. DiMatteo and Michel Cannarsa (eds) *Research Handbook on the Metaverse and Law* (Edward Elgar Publishing, Cheltenham, 2024) 118-157, 118).

86 Danique Knibbeler, Max Mohrmann and Sarah Zadeh, 'Privacy and security concerns in the metaverse' (www.nautadutilh.com, August 2022) <https://www.nautadutilh.com/en/insights/privacy-and-security-concerns-in-the-metaverse/> accessed 17 July 2025.

87 Xynogalas and Leiser (n 34) 99.

88 Koehler (n 67).

89 See Ljubisa Bojic, 'Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality?' (2022) *Eur J Futures Res* 10, 22.

90 Xynogalas and Leiser (n 34) 97.

91 Diletta De Cicco, James Downes and Charles Helleputte, 'No Children in the Metaverse? The Privacy and Safety Risks of Virtual Worlds (and How to Deal with Them)' In *Privacy Technologies and Policy: 11th Annual Privacy Forum, APF 2023, Lyon, France, June 1-2, 2023, Proceedings* (Springer-Verlag, Berlin, Heidelberg, 2023), 87-108, 97.

54 Given these limitations, exploring alternative legal grounds for data processing in the Metaverse becomes essential. One such ground, the performance of a contract under Article 6(1)(b) GDPR, may justify certain data uses. However, this basis introduces its own complications. Controllers must demonstrate that each processing operation is strictly necessary to fulfil a contractual obligation, aligning with users' reasonable expectations. They must also assess whether the terms themselves are fair and whether they disguise excessive data practices under the guise of contractual necessity, a task made even more difficult by the Metaverse's data-intensive architecture and fluid user engagement.⁹²

55 Moreover, even when relying on the performance of a contract or other legal bases under Article 6 GDPR, processing special categories of data remains particularly challenging. Such processing requires satisfying one of the specific exceptions enumerated in Article 9(2) GDPR, a threshold that significantly restricts the circumstances under which this sensitive data may be lawfully handled, underscoring the necessity for rigorous legal scrutiny.

IV. Territorial Scope of Data Regulations

56 Metaverses operate on a global scale, relying on the seamless flow of information across platforms, service providers and national borders. This global reach, combined with the involvement of numerous end-users, service providers, and diverse stakeholders, complicates the task of determining which legal frameworks apply to these virtual spaces. The result is often a cumulative layering of overlapping and intersecting regulations that must be reconciled simultaneously. The Metaverse's decentralised structure, extensive interoperability, and the current lack of tailored regulation only deepen this complexity.⁹³

57 Pinpointing users' locations within the Metaverse further obscures jurisdictional boundaries. Factors such as the physical location of the individual controlling an avatar, the avatar's position within the virtual environment, and the geographic

92 See European Data Protection Board, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms. 17 April 2024', paragraphs 41, 53 and 116. Available at https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

93 Schürmann Rosenthal Dreyer, 'The Metaverse: Data Protection in a New Virtual World | SRD' (www.srd-rechtsanwaelte.de, 15 June 2022) <https://www.srd-rechtsanwaelte.de/en/blog/metaverse-data-protection/> accessed 17 July 2025.

location of data servers all blur traditional notions of territoriality. As Metaverses develop, the question of which jurisdiction governs disputes involving avatars grows increasingly ambiguous,⁹⁴ especially when multiple service providers and virtual identities intersect.

- 58 Given that data protection laws safeguard fundamental rights that cannot be waived, contractual choice of law provisions are inherently limited in their reach.⁹⁵ For example, the GDPR applies extraterritorially to non-EU platforms and controllers processing the personal data of EU residents, whether by offering goods or services or monitoring behaviour within the Union. Moreover, operators cannot segregate EU users' data from that of other users to circumvent these obligations.⁹⁶ While contractual clauses may attempt to clarify the relationship between providers and users, their enforceability varies widely across jurisdictions, exposing providers to potential litigation in multiple fora.⁹⁷

V. Responsibility and Controllershship

- 59 The Metaverse complicates data protection compliance by dispersing personal data processing across layered infrastructures and interdependent actors. Interoperable architectures facilitate data flows across multiple actors, blurring the lines of legal accountability as information collected by one party circulates seamlessly across platforms, services and devices.
- 60 Compounding this complexity is the autonomous data collection by third-party developers, which further fragments control and complicates attribution. As the Metaverse deepens its reach, the web of stakeholders and interactions tightens, making the precise assignment of GDPR-defined data protection roles extraordinarily elusive.⁹⁸ Within this tangled ecosystem, joint controllership becomes the norm rather than the exception, as personal data typically flows through an interconnected chain of actors, spanning device manufacturers, platform operators, and third-party services.⁹⁹
- 61 Under the GDPR, a controller is the entity that determines the purpose ("why") and means ("how") of processing. In the Metaverse, controllers include a wide array of actors who collect or access data within virtual spaces (sometimes directly from users, other times from bystanders). While controllers shape the objectives and parameters of data processing, they may delegate implementation to processors.¹⁰⁰ They may include platform and service providers responsible for developing the infrastructure and devices that enable the Metaverse, and, in certain cases, individuals who interact within these environments as end-users.¹⁰¹ Broadly, controllers in the Metaverse can be classified into four main categories:
- 62 (1) Platform Operators/Administrators. These entities shape the Metaverse's architecture, policies, and user experience. They design and maintain the virtual environment and govern interactions within it, from user behaviour to content moderation. While the purpose and scope of data collection vary, they commonly focus on personalising experiences, strengthening security, and optimising the overall performance of metaverse platforms. Beyond data management, these operators play a crucial role in safeguarding Metaverse's security and stability by protecting it from disruptions, cyberattacks, and unauthorised access.
- 63 (2) Service Providers. These actors deliver a range of services within the Metaverse, ranging from e-commerce platforms and social interaction tools to content hosting environments. Their role extends beyond mere facilitation; by defining the purposes and means through which personal data is processed to enable these services, they assume significant control over user data.
- 64 (3) Third-Party Developers. Developers of games, applications, or immersive experiences in the metaverse environment may assume the role of data controllers when they independently collect and process personal information. Their role becomes especially significant when setting terms

94 Cheong (n 4) 471.

95 Jie (Jeanne) Huang, 'Applicable Law to Transnational Personal Data: Trends and Dynamics' (2020) 21 *German Law Journal* 1283, 1299.

96 Bristows (n 33).

97 Matthias Artzt and Gary Weingarden, 'Metaverse and Privacy' (2022) 15 *International In-House Counsel Journal* 59, 7763, 7765.

98 Koehler (n 67).

99 Guillaume Cuneson and Jennifer Calver, 'Metaverse Series #6: Data in the Metaverse – More Personal than Ever' (Techinsights Linklaters, 22 September 2022) <[https://](https://techinsights.linklaters.com/post/102hxlh/metaverse-series-6-data-in-the-metaverse-more-personal-than-ever)

techinsights.linklaters.com/post/102hxlh/metaverse-series-6-data-in-the-metaverse-more-personal-than-ever> accessed 17 July 2025.

100 See 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' (2020) https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf accessed 17 July 2025.

101 World Economic Forum and Accenture, 'Interoperability in the Metaverse: Briefing Paper' (World Economic Forum 2023) https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf accessed 20 July 2025.

of engagement or embedding data analytics within their tools, thereby shaping data collection and use.

- 65 (4) Users. End-users may also function as controllers, particularly when they generate content, interact with other participants, or manage their personal data across metaverse platforms. This role implies processing data about other users or bystanders, involving decisions about virtual interactions, data collection, and sharing.
- 66 Responsibility in the Metaverse depends on both functional positions and its structural form. In centralised platforms, operators exert significant control over architecture, data flows, and compliance, while service providers generally align with their policies. Third-party developers may act as data controllers or processors depending on the autonomy and scope of their data collection. In decentralised or hybrid systems, responsibilities are distributed across operators, providers, developers, and users, creating shared accountability and more complex governance arrangements.
- 67 Roles in virtual worlds are fluid and context-dependent, making it difficult to determine who qualifies as a controller, joint controller or processor under the GDPR.¹⁰² This uncertainty makes it harder to apply key data protection principles and can get in the way of users fully exercising their rights.
- 68 Despite these challenges, the responsibilities of actors within the Metaverse largely fall within existing regulatory frameworks. Platform operators, service providers, third-party developers, and even users can typically be classified under the GDPR's definitions of controllers, joint controllers, or processors, with comparable obligations arising under the Digital Services Act (DSA)¹⁰³ and the Digital Markets Act (DMA)¹⁰⁴ where applicable. Rather than requiring entirely new regulatory categories, these frameworks offer the tools to assign accountability, enforce obligations, and protect users' rights, provided regulators and stakeholders interpret and

apply the rules with attention to the Metaverse's distributed structures.

VI. Seamless Integration, Interoperability and Portability

- 69 Metaverse ecosystems encompass a mosaic of distinct systems and technologies, each shaped by different providers.¹⁰⁵ Frictionless movement within and between distinct metaverse platforms hinges on two interconnected challenges: seamless interoperability and effective data portability. Crossing these boundaries exposes users to a patchwork of technical standards, policies, and legal frameworks, complicating efforts to protect user control and ensure consistent safeguards.
- 70 Interoperability can be defined as the “ability to interact, exchange and make use of data and resulting information to enable movement, transactions and participation across systems, platforms, environments and technologies”.¹⁰⁶ Often termed “cross-metaverse interoperability,” it ensures a continuous user experience,¹⁰⁷ minimising interruptions and discontinuities as individuals transition between virtual worlds.
- 71 Complementing interoperability, the right to data portability under Article 20 GDPR empowers data subjects to obtain and transfer their personal data between service providers.¹⁰⁸ Within the Metaverse, this right enhances user autonomy by enabling access, reuse, and transfer of data across platforms, thereby fostering a more user-centric ecosystem. To achieve these goals, common technical standards, such as “standard data formats”,¹⁰⁹ are necessary, which mitigate vendor lock-in, i.e., situations where users are confined to a single metaverse platform and unable to move their personal data easily,¹¹⁰ limiting

¹⁰² Knibbeler et al. (n 86).

¹⁰³ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277/1 (27 October 2022) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065>.

¹⁰⁴ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265/1 (12 October 2022) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R1925>.

¹⁰⁵ Bristows (n 33).

¹⁰⁶ World Economy Forum and Accenture (n 101).

¹⁰⁷ Taotao Li and others, ‘MetaOpera: A Cross-Metaverse Interoperability Protocol’ (2023) 30 *IEEE Wirel. Commun.* 5, 136-143, 136.

¹⁰⁸ Sanna Toropainen, ‘The right to data portability in the fair data economy – extending the right of individuals to benefit from managing their data’ (2023) Sitra https://media.sitra.fi/app/uploads/2023/09/sitra_the-right-to-data-portability-in-the-fair-data-economy-final.pdf accessed 20 July 2025, 13.

¹⁰⁹ Franklyn Ohai, ‘The Threat Landscape of Extended Reality: Beyond Privacy and Data Protection’ (www.law.kuleuven.be, 21 November 2023) <https://www.law.kuleuven.be/citip/blog/the-threat-landscape-of-extended-reality-beyond-privacy-and-data-protection/> accessed 20 July 2025.

¹¹⁰ Knibbeler et al. (n 86).

consumer choices.¹¹¹ Currently, switching between metaverse ecosystems is difficult for individuals, as each setting has its own protocols, and there is limited interoperability.¹¹²

- 72 Interoperability challenges in centralised metaverse platforms could find a more natural remedy in competition law. Many of the largest platforms act as digital gatekeepers under the DMA, granting regulators the authority to enforce openness and, ultimately, enable meaningful data portability. In this way, market-oriented interventions can complement GDPR safeguards, addressing technical bottlenecks and structural barriers.

VII. Data Security Risks

- 73 Distributed, sensor-driven digital ecosystems amplify cybersecurity risks due to the vast quantities of information harvested by interconnected devices and embedded sensors,¹¹³ particularly with respect to the availability, resilience, and confidentiality of personal data processed.¹¹⁴ The very attributes that define these spaces, such as social interaction, immersive engagement, real-world simulation and scalability, intensify these data security concerns.¹¹⁵ Threats arise across multiple layers, encompassing risks related to data inputs, processing, outputs, user interactions and device operation.¹¹⁶
- 74 The scope and complexity of these risks depend on factors such as the platform's architecture (centralised or decentralised), the nature of processing operations and the types of devices employed. Integrating data from the IoT further enlarges the potential attack surface.¹¹⁷ These vulnerabilities can manifest as personal information leakage, eavesdropping, data theft, unauthorised access, phishing, data injection, broken authentication, insecure design and related exploits.¹¹⁸
- 75 The fluid and real-time exchanges on which metaverse services depend make safeguarding

personal information especially challenging.¹¹⁹ Protections at the device, software component, or unit level, while necessary, are insufficient when applied in isolation, particularly in decentralised systems where fragmented control can create gaps.

VIII. Exercise of Data Subjects' Rights in the Immersive Digital World

- 76 As noted earlier, Metaverse dissolves geographical boundaries, bringing disparate data protection regimes into constant collision. Within these varying regimes, each with its own regulatory approaches, data protection rights and obligations can diverge significantly, depending on the specific data protection law(s) applicable to a given case.¹²⁰ The result is a fragmented legal terrain where procedural requirements, substantive protections and remedies differ sharply. Opaque and overbroad privacy policies deepen the uncertainty, leaving users without a clear sense of how their rights apply in practice.¹²¹
- 77 Identity in virtual spaces is often fluid, with users operating through pseudonyms or avatars. In certain cases, the tenuous link between virtual personas and real-world identities can make it difficult to verify requests under the GDPR or other regimes, and to respond appropriately.
- 78 The governance models of decentralised metaverse settings and distributed ledger technologies introduce further obstacles. Without a central authority, responsibility could splinter, and accountability dissipate. Beyond joint controllership, pinpointing who bears legal liability for privacy breaches becomes a daunting task. Accessing, rectifying or erasing personal data can be particularly difficult when it is stored in encrypted or hashed form. Finally, users might face significant obstacles in identifying or contacting metaverse data controllers or processors, who may obscure their identities by operating through intermediaries or proxies.¹²²

111 European Parliamentary Research Service (n 6).

112 Toropainen (n 108) 28.

113 Chris Warin and Delphine Reinhardt, 'Vision: Usable Privacy for XR in the Era of the Metaverse' in *Proceedings of the 2nd European Symposium on Usable Security (EuroUSEC)* (Association for Computing Machinery, 2022), 111-116, 113.

114 Agencia Española de Protección de Datos (n 7).

115 Yan Huang and others, 'Security and Privacy in Metaverse: A Comprehensive Survey' (2023) 6 *Big Data Mining and Analytics* 2, 234-247, 235.

116 Warin and Reinhardt (n 113).

117 IBM Institute for Business Value, 'Seven Bets' (IBM Corporation 2023) <https://www.ibm.com/downloads/cas/GN7B276L> accessed 20 July 2025, 26.

118 Huang et al. (n 115).

119 Dwivedi et al. (n 9) 8.

120 Artzt and Weingarden (n 97).

121 Natalia Menéndez González and Efe Bozkir, 'Eye-tracking Devices for Virtual and Augmented Reality Metaverse Environments and Their Compatibility with the European Union General Data Protection Regulation' (Robert Schuman Centre for Advanced Studies, Centre for a Digital Society, Working Paper RSC 2023/69, 2023) https://cadmus.eui.eu/bitstream/handle/1814/76162/RSC_WP_2023_69.pdf?sequence=1&isAllowed=y accessed 20 July 2025.

122 Artzt and Weingarden (n 97). "[I]n the operation of the Metaverse, adherence to the rights of the individuals

F. Can Data Protection by Design Truly Work in the Metaverse?

79 Previous sections have revealed how the Metaverse exposes deep tensions within established data protection frameworks, particularly the GDPR's purpose limitation and data minimisation principles. These principles are designed to impose meaningful limits on data collection and processing, yet the Metaverse's immersive, continuous, and highly interconnected data flows challenge their practical enforceability. Far from isolated transactions, data exchanges in these environments are dynamic and layered, complicating efforts to apply regulatory safeguards. The result is a growing friction between the expansive data ambitions of metaverse technologies and the foundational rights-based limits that seek to govern them.

80 Data Protection by Design theoretically offers a pathway to align rapid technological innovation with privacy imperatives; however, the Metaverse's architecture exposes significant fault lines in this ideal. Rather than reflecting a genuine integration of DPbD principles, current systems risk reducing them to performative gestures that obscure deeper regulatory and technical shortcomings. The continuous flow of data, the shifting nature of user identities, and the complex interactions across multiple platforms undermine efforts to embed privacy from the outset. Fragmented governance further hinders the coordination needed for a unified data protection approach.

I. Integrating Privacy into the Core: The Strategic Role of Data Protection by Design

81 DPbD is a forward-looking and comprehensive strategy that embeds privacy into every layer of the system's architecture. It requires elevating privacy beyond an afterthought to a core tenet that shapes the development of information systems, technologies, and data management processes, thereby enhancing regulatory flexibility.¹²³ This approach, paired with data protection by default,

embraces a risk-based framework,¹²⁴ that tailors safeguards to the nature, scope, and potential impact of data processing activities.

82 Fundamentally, DPbD recognises that processing of personal data transcends mere technical challenges, encompassing systemic dimensions of governance, architecture, and user empowerment. Data protection and security considerations should be incorporated throughout all stages of processing, starting from the earliest phases of development,¹²⁵ enable data processing stakeholders to effectively manage the risks inherent in these operations, being far more effective than retrofitting these measures after a product or service is built.¹²⁶

83 The integration of data protection requirements from the outset and as a default, as mandated by Article 25 of the GDPR, represented an important advancement in the reform of the European personal data framework.¹²⁷ The significance of data protection by design in this framework lies not only in its cross-cutting role as a guiding principle,¹²⁸ but also in its status as an enforceable legal obligation, exemplifying what is termed "legal protection by design."¹²⁹ Its purpose is to embed legal safeguards

124 Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford University Press, Oxford, 2020), 155.

125 Marco Almada, Juliano Maranhao and Giovanni Sartor, 'Art. 25. Data protection by design and by default', in Indra Spiecker gen. Döhmman, Vagelis Papakonstantinou, Gerrit Hornung and Paul de Hert (eds), *General data protection regulation : article-by-article commentary* (Nomos, Beck, Hart Publishing, 2023), 581-582.

126 European Union Agency for Cybersecurity, 'Privacy and Data Protection by Design' (2015) <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> accessed 23 July 2025, 11.

127 Christopher Kuner, Lee A Bygrave, and Christopher Docksey, 'Background and Evolution of the EU General Data Protection Regulation (GDPR)', in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, Oxford, 2020), 26. Article 25 of the GDPR is a new provision under EU law; the 1995 Data Protection Directive, which preceded the GDPR, did not specifically address this concept, although it briefly mentions the idea in Recital 46 (Christina Michelakaki and Sebastião Barros Vale, 'Unlocking Data Protection by Design & By Default: Lessons from the Enforcement of Article 25 GDPR' (Future of Privacy Forum 2023) <https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf> accessed 25 July 2025).

128 "A broad vision of Article 25(1) transforms it into a kind of catch-all provision, scooping up anything omitted from other, more specific sections of the GDPR" (Ari Ezra Waldman, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53 *Cornell International Law Journal* 1, 147-167, 164).

129 Mireille Hildebrandt and Laura Tieleman, 'Data Protection

had not been feasible in some instances [for example] due to difficulties in identifying the parties responsible for data security" (Vibhushinie Bentotahewa and others, 'Privacy and Security Landscape of Metaverse', in Nitin Naik and others (eds) *Advances in Computational Intelligence Systems: Contributions Presented at the 22nd UK Workshop on Computational Intelligence (UKCI 2023), September 6-8, 2023, Birmingham, UK* (Springer, Cham, 2024), 407).

123 Avner Levin, 'Privacy by Design by Regulation: The Case Study of Ontario' (2018) 4 *CAN. J. COMP. & CONTEMP. L.* 115.

directly into the information and communication technology infrastructure that supports data-driven environments.¹³⁰ In this line, DPbD underscores the importance of recognising the significant and inherent regulatory potential embedded within the architecture of information systems.¹³¹

- 84 This concept typically involves minimising data use while enhancing security, restricting access, and limiting data distribution.¹³² Framed in this manner, the duties of data protection by design require the systematic application of fundamental principles such as transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability, as set forth in Article 5 and Recital 39 GDPR.¹³³
- 85 Data Protection Impact Assessments (DPIAs), mandated by Article 35 GDPR, reflect the proactive spirit of DPbD. They systematically identify and manage risks, implementing safeguards before harm occurs. DPIAs offer a structured process to evaluate the necessity, proportionality, and potential risks of data processing,¹³⁴ supporting compliance,¹³⁵ and

providing a clear framework for managing high-risk activities in accordance with GDPR requirements.

II. Scaling Data Protection by Design in the Metaverse: Key Challenges

- 86 In the Metaverse, implementing DPbD is not a procedural formality; it is a contested issue where technical, legal, and governance dimensions converge. Metaverse data fabrics strain governance structures, expose weak points in infrastructure, and erode user control. The velocity and granularity of these virtual worlds outpace traditional safeguards, demanding a shift to a holistic framework. This transformation calls for more than patchwork fixes, requiring an ecosystem-wide strategy. Against this complex backdrop, three central challenges emerge as decisive factors shaping the path forward:
- 87 (1) Gatekeepers and Platform Authority. The operators of metaverse platforms occupy a position of unparalleled control. They do not simply host virtual environments; they architect the rules, set the technical boundaries, and determine the very conditions under which interaction and data flows occur. Their role extends to shaping every stage of data handling: from limiting collection to what is strictly necessary, to embedding advanced safeguards such as state-of-the-art encryption and privacy-preserving architectures, including blockchain-based solutions.¹³⁶ In theory, such control could enable a rigorous application of DPbD, integrating privacy safeguards into every layer of the system from inception.
- 88 In practice, however, these gatekeepers often operate under economic incentives that conflict with such goals. The difficulty lies not merely in technical implementation but in a structural dilemma: the very actors expected to integrate data protection safeguards are also those with the strongest interest in maximising data extraction. Their business models thrive on pervasive collection, behavioural profiling, and the monetisation of user engagement, practices that directly undermine data minimisation principles. Proprietary architectures and closed ecosystems entrench these dynamics,¹³⁷ consolidating control over design choices. When flaws arise, this centralised control acts as a force multiplier, allowing shortcomings to cascade across vast portions and data controllers of the Metaverse,

by Design and Technology Neutral Law' (2013) 29 *Computer Law & Security Review* 5, 509-521, 516.

- 130 Mireille Hildebrandt, 'Code Driven Law. Scaling the Past and Freezing the Future', in Simon Deakin and Christopher Markou (eds), *Is Law Computable?: Critical Perspectives on Law and Artificial Intelligence* (Hart Publishing, 2020), 67-84, 82.
- 131 Lee A. Bygrave, 'Article 25 Data protection by design and by default', in Christopher Kuner, and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, Oxford, 2020), 573.
- 132 Kostina Prifti and others, 'Regulation by Design: Features, Practices, Limitations, and Governance Implications' (2024) 34 *Minds & Machines* 2, 13.
- 133 European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020) Version 2.0 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf accessed 22 July 2025.
- 134 De Cicco et al. (n 91) 94.
- 135 Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, WP 248 rev 01, adopted 4 April 2017 <https://ec.europa.eu/newsroom/article29/items/611236> accessed 8 August 2025, 4.

136 Artzt and Weingarden (n 97) 7767.

137 Carlos Cantú, Cecilia Franco and Jon Frost, The economic implications of services in the metaverse (BIS Papers No 144, Bank for International Settlements February 2024) 21 <https://www.bis.org/publ/bppdf/bisap144.pdf> accessed 8 August 2025.

becoming deeply ingrained in its infrastructure and making remediation far more complex.

- 89 Additionally, dominant platforms may employ lock-in strategies to establish proprietary ecosystems that restrict users' ability to transfer data, assets, or identities across services. Several competing metaverse platforms appear increasingly monopolistic,¹³⁸ which may further reinforce these barriers by imposing closed standards and limiting open collaboration. This concentration of power risks consolidating control over data flows and complicating efforts to achieve comprehensive data protection.
- 90 (2) The Decentralisation Paradox. The shift to decentralised architectures, often heralded as a pathway to greater user control and resilience, introduces profound complexities for DPbD. Unlike centralised systems, decentralisation disperses control across a multitude of actors, devices, and services. This fragmentation complicates the comprehensive implementation of consistent safeguards, undermining the necessary holistic approach to privacy. As a result, it fosters a patchwork of fragmented solutions, each addressing isolated aspects, which perpetuates disintegration and weakens the overall effectiveness of data protections.
- 91 The challenge lies in reconciling the collaborative, interoperable nature of federated networks with the stringent demands of data privacy preservation. Every node in the network, whether a metaverse service provider, device manufacturer, or software developer acting as a data controller, must implement protection measures that adhere to shared standards. However, the absence of a centralised authority complicates coordination and dilutes accountability. The dispersion of responsibility creates vulnerabilities in privacy protections, eroding trust and exposing users to heightened risks. Moreover, it is important to recognise that many technology developers who contribute to the ecosystem but do not qualify as data controllers remain outside the direct scope of DPbD obligations,¹³⁹ leaving additional blind spots in data protection.
- 92 (3) The Regulatory Maze in the Virtual World. The Metaverse's borderless nature clashes head-on with a patchwork of privacy regimes. While this digital frontier transcends traditional jurisdictional boundaries, metaverse stakeholders and data controllers remain subject to diverse and often conflicting legal frameworks tied to users' locations. As a result, metaverse developers must tailor their

services to comply with the specific laws and regulations applicable in each country or region.¹⁴⁰ This dynamic exposes a fundamental tension: the Metaverse aspires to offer seamless, global interaction, whereas it remains constrained by the territorial reach of national laws.

- 93 Multiple privacy laws may simultaneously apply to the same data or individual,¹⁴¹ imposing varying obligations regarding transparency, lawfulness, user rights, breach notifications, and cross-border data transfers. This multiplicity makes universal terms and conditions unlikely,¹⁴² particularly when virtual worlds are designed primarily to comply with the laws of their gatekeepers or main operators' home countries. The underlying infrastructure and devices often fail to accommodate the diverse regulatory demands of all jurisdictions where these environments are accessed.
- 94 This mosaic turns DPbD into a daunting puzzle. Consider the United States, where privacy by design remains more a whisper than a mandate, though rising calls for risk assessments signal a subtle shift. Whether these assessments will fully capture the comprehensive spirit of DPbD is yet to be seen.¹⁴³ Meanwhile, regulatory bodies like the Federal Trade Commission hint at a growing appetite for integrating privacy principles upstream.¹⁴⁴

III. Data Protection by Design at the System Level

- 95 Scaling DPbD in data-saturated ecosystems defies simple solutions. The sheer density and interconnectedness of data streams across devices, platforms, and services expose the limits of isolated technical patches. This necessitates an integrated, ecosystem-level overhaul, one that fundamentally shapes software design patterns, infrastructure

140 Chuan Chen and others, 'Privacy computing meets metaverse: Necessity, taxonomy and challenges' (2024) 158 *Ad Hoc Networks*, 11.

141 Artzt and Weingarden (n 97).

142 Norton Rose Fulbright, 'The Metaverse: The evolution of a universal digital platform' (www.nortonrosefulbright.com, November 2022) <https://www.nortonrosefulbright.com/en-nl/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform> accessed 8 August 2025.

143 Artzt and Weingarden (n 97) 7767.

144 Richmond Y. Wong and Deirdre K. Mulligan, 'Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery, New York, 2019) Paper No 262, 1.

138 Nick Munn and Dan Weijers, 'The Real Ethical Problem with Metaverses' (2023) 5 *Frontiers in Human Dynamics* 1226848, 3.

139 Hildebrandt and Tielemans (n 129) 519.

architecture, and the deployment of privacy-enhancing technologies.¹⁴⁵

- 96 On a broader scale, modular and composable system architectures are crucial to enable privacy-preserving components to be updated or replaced as new threats emerge, facilitating ongoing adaptability and resilience. Integrating privacy into the underlying infrastructure through secure communication protocols and identity management systems ensures that protection is not an afterthought but a core design principle.
- 97 At a granular level, practical measures include empowering users with meaningful controls to limit data exposure, even when this might affect certain facets of user experience.¹⁴⁶ Features such as automatic blurring of bystanders, selective data obfuscation,¹⁴⁷ and real-time consent management help reduce inadvertent exposure within immersive environments. Furthermore, fine-grained access controls, data minimisation protocols, and encryption techniques for data at rest and in transit serve as key tools to safeguard sensitive information.
- 98 Equally critical are governance mechanisms that extend beyond technical solutions. Continuous and iterative DPIAs integrated early and throughout the development lifecycle are essential to identify, evaluate, and mitigate risks as these complex systems evolve. Transparent accountability frameworks must clearly allocate responsibilities across a wide range of stakeholders including platform operators, service providers, device manufacturers, and third-party developers. Without such clarity, the distributed and interconnected nature of the Metaverse risks creating regulatory blind spots where protections falter. Governance in this space must grapple with the complexity of overlapping jurisdictions, diffuse authority, and competing interests, ensuring that fragmentation does not translate into loopholes that erode privacy and user trust.
- 99 However, a critical question persists: can immersive architectures undergo fundamental redesigns at this stage? Keeping in mind the technological momentum and current maturity of these systems, some room for adjustment still exists. Although still in its developmental phase, the Metaverse is expected to evolve rapidly,¹⁴⁸ characterised by speculative features, uneven implementation, and the absence of a fully established business model.¹⁴⁹ At the same time, rapid technological advances continue to outpace regulatory efforts, making data protection a moving target rather than a fixed guarantee. In this

shifting landscape, it is unclear whether integrating DPbD in virtual spaces remains more an aspirational ideal than an operational reality, transcending rhetoric to deliver meaningful, lasting safeguards.

- 100 Centralised metaverse platforms could provide a conducive setting for implementing DPbD duties. Their cohesive structures may allow a single actor to integrate privacy considerations consistently, coordinate data management, and deploy protective technologies across the platform. Such oversight can make monitoring and auditing more straightforward, potentially enabling faster detection and resolution of data protection issues. This apparent advantage, however, comes with a trade-off: concentrating control generates points of failure and structural vulnerabilities that require careful management.
- 101 Moreover, while centralised architectures can support more integrated privacy measures at the level of structures and processes, they also risk entrenching or exacerbating data protection challenges that remain unaddressed in the earliest design stages. Absent deliberate foresight, such systems risk reproducing or magnifying data protection gaps, underscoring that structural coherence alone cannot secure genuine compliance with the DPbD principle.
- 102 A clear example is Horizon Worlds, a Meta's virtual reality social platform.¹⁵⁰ It allows users to create, explore, and interact in three-dimensional virtual spaces through avatars.¹⁵¹ Within the platform, users can build their own worlds, design games, and share experiences, engaging with others in real time. As a centralised system, control over servers, governance, rules, and most data processing remains with Meta, limiting the degree of influence users have over how the platform operates.¹⁵²
- 103 The platform has attracted attention in debates surrounding privacy, data protection, and interoperability, particularly due to its extensive collection of behavioural and spatial data. These practices have been identified as posing potential

145 European Union Agency for Cybersecurity (n 126).

146 Olaizola Rosenblat (n 3) 18.

147 Ibid.

148 Arismendy Mengual (n 13).

149 Wang et al. (n 65) 14673.

150 Meta Horizon (Web Page) https://horizon.meta.com/?locale=en_US accessed 20 January 2026. Meta Horizon <https://horizon.meta.com/?locale=en_US> accessed 20 January 2026.

151 Kethryn Marie Protz, *Walk on the Metaverse Side: Data Protection in the Virtual Worlds* (Master of Science in Law, Digital Innovation and Sustainability, LUISS Guido Carli University 2023) page 11 https://tesi.luiss.it/37451/1/630803_PROTZ_KETHRYN%20MARIE.pdf accessed 20 January 2026.

152 Shymaa Ararat, 'Open vs Closed Metaverses: Decentraland & Horizon Worlds as Featured Examples' *Medium* (9 April 2025) < <https://medium.com/%40shymaa.ararat/open-vs-closed-metaverses-decentraland-horizon-worlds-as-a-featured-examples-2501923286b6>> accessed 20 January 2026.

risks to users' rights and freedoms, given the nature, context, and purpose of the data processing.¹⁵³ Horizon Worlds actively records user behaviour, including audio logs, as part of its data retention policy,¹⁵⁴ and it has the capacity to monitor users invisibly in real time to detect potential rule violations.¹⁵⁵

104 Concerns have also been raised regarding the platform's priorities, emphasising user growth, while safety and privacy considerations (such as protecting children) were managed primarily as potential liabilities rather than core design principles.¹⁵⁶ The data collected by Meta could be leveraged to enhance its metaverse offerings for advertisers and business partners, raising additional questions about the commercialisation of user information.¹⁵⁷ A 2025 complaint to the U.S. Federal Trade Commission alleges that Meta allowed children under 13 to access Horizon Worlds, collected their personal data without parental consent, and thereby exposed them to potential harm under the Children's Online Privacy Protection Act (COPPA).¹⁵⁸

G. Conclusion

105 The Metaverse is not a single platform or isolated enclave. It is an interconnected ecosystem of applications, services, and virtual environments.

It includes both centralised and decentralised architectures, allowing users to interact with one another and with data-intensive technologies in real time. It does not exist as a separate digital realm or purely fictional space. Instead, it represents an evolution of the Web, building on established digital practices while expanding interactions and data exchanges in ways that intensify existing governance challenges.

106 The operational reality of the Metaverse depends on extensive and persistent information flows, collecting and generating massive volumes of data. Its infrastructural dynamics and processing logics make it more difficult to apply fundamental data protection principles, such as purpose limitation and data minimisation. Fragmented regulations and inconsistent standards further exacerbate these risks.

107 Data Protection by Design provides a clear framework for addressing these challenges. Integrating privacy considerations into every stage of system development transforms personal data protection from an optional feature into a structural safeguard. This approach (often described as "techno-regulation" or "legal by design") treats technology not merely as a tool but as a force that shapes legal and ethical practices.¹⁵⁹ It promotes proactive risk management, minimal data collection, and protective measures throughout the lifecycle of a system,¹⁶⁰ demonstrating the regulatory potential embedded within digital infrastructures.¹⁶¹

108 Centralised metaverse platforms can make this approach easier to implement because a single authority or small governing group can enforce privacy rules consistently, coordinate data handling, deploy privacy-enhancing technologies, and monitor compliance across the platform. However, concentrated control carries inherent risks. Single points of failure can amplify threats to fundamental rights, and the sheer scale and complexity of the Metaverse often exceed the capacity of any single authority to maintain comprehensive protection. Structural redesigns are rarely feasible amid

¹⁵³ Protz (n 151) 43.

¹⁵⁴ Aryabrata Basu, Mohammad Jahed Murad Sunny and Jayasri Sai Nikitha Guthula, 'Privacy Concerns from Variances in Spatial Navigability in VR' (arXiv:2302.02525, preprint, 6 February 2023) <https://arxiv.org/abs/2302.02525> accessed 21 January 2026.

¹⁵⁵ Ben Lang, 'Facebook Horizon Can Invisibly Observe Users to Spot Rule Violations' Road to VR (28 August 2020) <https://www.roadtovr.com/facebook-horizon-privacy-monitoring-moderation/> accessed 22 January 2026.

¹⁵⁶ <https://www.businessinsider.com/meta-horizon-worlds-child-safety-whistleblower-ftc-fairplay-2025-4> See Jyoti Mann and Pranav Dixit, 'Meta Whistleblower Claims the Company Put Profit over the Safety of Children in Horizon Worlds' *Business Insider* (10 April 2025) <<https://www.businessinsider.com/meta-horizon-worlds-child-safety-whistleblower-ftc-fairplay-2025-4>> accessed 21 January 2026.

¹⁵⁷ Brooks Canavesi, 'The Foundation of the Metaverse: Centralization Versus Decentralization' ATD Blog (2 February 2022) <https://www.td.org/content/atd-blog/the-foundation-of-the-metaverse-centralization-versus-decentralization> accessed 24 January 2026.

¹⁵⁸ Fairplay, Complaint against Meta filed at FTC alleging widespread Horizon Worlds child privacy violations (Press release, 10 April 2025) <https://fairplayforkids.org/complaint-against-meta-filed-at-ftc-alleging-widespread-horizon-worlds-child-privacy-violations/> accessed 24 January 2026.

¹⁵⁹ Carlotta Rigotti and Gianclaudio Malgieri, *Sexual Violence and Harassment in the Metaverse: A New Manifestation of Gender-Based Harms* (The Alliance for Universal Digital Rights (AUDRI), Equality Now and The International Observatory on Vulnerable People in Data Protection (Vulnera) 2024) <<https://audri.org/wp-content/uploads/2024/04/EN-AUDRI-Sexual-violence-and-harassment-in-the-metaverse-03.pdf>> accessed 6 August 2025.

¹⁶⁰ Agencia Española de Protección de Datos, 'Guía de Privacidad desde el Diseño' (2019) <<https://www.aepd.es/guías/guia-privacidad-desde-diseno.pdf>> accessed 5 August 2025, 6.

¹⁶¹ Bygrave (n 131).

rapid technological development and commercial pressures. This tension underscores a persistent trade-off: centralised systems enable more effective oversight but concentrate power, whereas decentralised systems disperse risk but complicate enforcement.

- 109** Although the temptation exists to craft a specialised legal regime for the Metaverse, such a measure appears unnecessary. Existing regulatory instruments (including the DMA and DSA) already provide the tools to address its key challenges. Platforms can integrate privacy protections directly into their architectures, operationalising DPbD to make privacy a structural feature rather than an afterthought. At the same time, these frameworks empower regulators to monitor compliance, enforce obligations, and maintain oversight across platforms. Merging technology/application-level protections with regulatory oversight, this approach addresses ongoing privacy and governance challenges from the broader Web, while respecting the limits of both centralised and decentralised control.
- 110** The path forward in the Metaverse lies not in new rules, but in how we apply and shape the ones we already have. Metaverse platforms and applications must make privacy a structural component, while regulators must use established instruments to enforce compliance and guide development. Success will depend on a dynamic interplay: technological design that anticipates risk, and technology-neutral legal frameworks designed to adapt to innovation.