



D7.5: Second Policy Brief

Revision: v.1

Work package	WP 7
Task	Task Number 7.2
Due date	31/10/2025
Submission date	31/10/2025
Deliverable lead	The Lisbon Council asbl
Version	1.0
Authors	Alessandro Paciaroni (The Lisbon Council) Francesco Mureddu (The Lisbon Council) Francesco Molinari (The Lisbon Council) Arno Laeven (The Lisbon Council)
Reviewers	POLIMI TRUST-IT
Abstract	This deliverable presents the second set of OPENVERSE policy briefs, which explore how regulatory sandboxes and trust-by-design principles can guide Europe’s leadership in virtual worlds and immersive technologies. It proposes concrete mechanisms - such as a “28th Regime” sandbox and EU label for Trust Tools - to foster innovation while safeguarding rights, transparency, and interoperability. The resulting framework aims to ensure that Europe’s immersive digital future remains open, ethical, and globally competitive.
Keywords	Regulatory sandboxes; trust-by-design; design principles; immersive technologies; policy; 28 th regime; virtual worlds



Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	01/10/2025	Table of Content	Alessandro Paciaroni (the Lisbon Council)
V0.2	28/10/2025	Introduction, Methodology, Conclusions and Appendixes	Alessandro Paciaroni (the Lisbon Council)
V0.3	30/10/2025	Appendixes	Alessandro Paciaroni (the Lisbon Council)
V0.4	31/10/2025	Policy Briefs	Francesco Molinari, Arno Laeven, Alessandro Paciaroni, Francesco Mureddu (the Lisbon Council)
V0.8	31/10/2025	Complete version ready for final review	Alessandro Paciaroni (the Lisbon Council)
V0.9	31/10/2025	Final internal review	John Favaro (Trust-IT)
V1	31/10/2025	Ethical Sign-off	Fabio Perossini, Alessandro Paciaroni

DISCLAIMER



**Funded by
the European Union**

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

Funded by the European Union (OPENVERSE, 101135701). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

COPYRIGHT NOTICE

© 2023 - 2026 OPENVERSE

Project funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project’s page)	
SEN	Sensitive, limited under the conditions of the Grant Agreement	



**Funded by
the European Union**

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Classified R-UE/ EU-R	<i>EU RESTRICTED under the Commission Decision No2015/ 444</i>	
Classified C-UE/ EU-C	<i>EU CONFIDENTIAL under the Commission Decision No2015/ 444</i>	
Classified S-UE/ EU-S	<i>EU SECRET under the Commission Decision No2015/ 444</i>	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.

EXECUTIVE SUMMARY

This deliverable, D7.5: Second Policy Brief, documents the research and participatory processes that led to the development of two complementary policy briefs under the OPENVERSE project that are here grouped in D7.5: Regulatory Sandboxes for Virtual Worlds Innovation: A Framework for EU Leadership and Trust Tools for Immersive Technologies. Together, these briefs advance a coherent European approach to the governance of immersive and virtual environments, aligning innovation with trust, ethics, and human-centric values.

Through a combination of desk research, stakeholder interviews, and policy-prototyping sessions - culminating in the high-level policy dialogue *To Trust or Not to Trust? How to Build a Trust-by-Design Architecture for Europe* - the project identified actionable policy pathways to support experimentation and cross-border cooperation. The first brief outlines how regulatory sandboxes can serve as agile governance instruments to test and scale innovation responsibly across the EU, proposing the creation of a “28th Regime” sandbox to enable pan-European experimentation. The second brief presents a Trust-by-Design Framework and introduces EU Trust Tools Sandboxes for testing interoperable identity, consent, and accountability mechanisms in immersive environments.

Together, these briefs propose a blueprint for a trustworthy, inclusive, and competitive European OpenVerse, where immersive innovation strengthens democratic values, market fairness and digital sovereignty.

TABLE OF CONTENTS

Disclaimer.....	2
Copyright notice.....	2
1 INTRODUCTION.....	9
2 METHODOLOGY.....	10
The policy dialogue: An EVIDENCE-BASED POLICY debate	10
The methods: Policy prototyping.....	10
3 POLICY BRIEF 1.....	12
3.1 Regulatory Sandboxes for Virtual Worlds Innovation: A Framework for EU Leadership	12
Key Takeaways	12
Urgency 13	
Expected readership	13
3.2 Introduction: The Promise and Peril of Virtual Worlds	13
3.3 THE REGULATORY CHALLENGE: SANDBOXES AS CATALYSTS FOR RESPONSIBLE INNOVATION IN THE EUROPEAN METAVERSE	15
3.4 NAVIGATING THE COMPLEXITIES: EXAMPLES OF (UN)EFFECTIVE INTERPLAYS BETWEEN VIRTUAL WORLDS AND THE REGULATORY FRONTIER.....	19
3.5 Designing Sandboxes for Virtual Worlds	25
3.6 Conclusions and Recommendations.....	31
4 POLICY BRIEF 2.....	34
4.1 Trust Tools for Immersive Technologies.....	34
5 CONCLUSIONS.....	52
6 ETHICS COMPLIANCE SIGN-OFF AND PUBLIC BRIEF DPIA	53
6.1 Ethics Compliance Sign-Off.....	53
6.2 Mitigation Actions Required	53
6.3 Overall Ethical Acceptability Evaluation	53
6.4 Public Brief Data Protection Impact Assessment (DPIA)	53
7 APPENDIX A	58
8 APPENDIX B	60
9 APPENDIX C	63
10 D. GLOSSARY OF USED TERMS	66
11 E. COMPARATIVE TABLE: SANDBOX MODELS IN EU VS. GLOBAL JURISDICTIONS	67
12 F. METHODOLOGY FOR CASE STUDY SELECTION.....	69
13 G. EUROPEAN STATE OF THE ART.....	70
14 H. INITIAL SET OF CASE STUDIES	72

15	I. EXPERT INTERVIEW SCRIPT	94
16	J. SELECTED FEEDBACK RECEIVED FROM INTERVIEWED EXPERTS	101
17	K COMPARATIVE TABLE OF REGULATIONS AND STRATEGIES REGARDING IMMERSIVE TECHNOLOGIES IN THE WORLD.....	106
18	L. INTERVIEW QUESTIONS	109

ABBREVIATIONS

AI	Artificial Intelligence
AR	Augmented Reality
AR/VR	Augmented Reality / Virtual Reality
BC	Blockchain
CORDIS	Community Research and Development Information Service
DAO	Decentralised Autonomous Organisation
DLT	Distributed Ledger Technology
DSA	Digital Services Act
DMA	Digital Markets Act
DID	Decentralised Identifier
EC	European Commission
EDPB	European Data Protection Board
EIC	European Innovation Council
EID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services
EU	European Union
EUBOF	EU Blockchain Observatory and Forum
GDPR	General Data Protection Regulation
GFIN	Global Financial Innovation Network
IPFS	InterPlanetary File System
MiCA	Markets in Crypto-Assets Regulation
MV	Metaverse
NFT	Non-Fungible Token
OECD	Organisation for Economic Co-operation and Development
R&D	Research and Development
SME	Small and Medium-sized Enterprise

TCP	Transmission Control Protocol
VR	Virtual Reality
VW	Virtual Worlds
WCAG	Web Content Accessibility Guidelines
WP	Work Package
XR	Extended Reality
XRSI	XR Safety Initiative

1 INTRODUCTION

This deliverable reports on the process that led to the development of *OpenVerse* Policy Briefs No. 2 and No. 3, which explore two complementary pillars of Europe's virtual worlds strategy: **trust** and **regulatory sandboxes**.

The final recommendations presented in those briefs were refined through an iterative process combining desk research, qualitative data analysis and an evidence-based **policy dialogue**, convened on 27 October 2025 under the title *To Trust or Not to Trust? How to Build a Trust-by-Design Architecture for Europe*.

This document summarises that process and shows how the dialogue's outcomes and the policy-prototyping session directly informed the two policy briefs, ensuring that their recommendations are not only theoretically sound but also practically tested and co-created with stakeholders.

2 METHODOLOGY

The OpenVerse methodological approach links **policy research** with **participatory validation**. The two policy briefs formed the analytical base, while the policy dialogue and its embedded policy-prototyping session provided the participatory design and validation.

This combination ensured a robust cycle of *analysis* → *co-design* → *validation* → *refinement*.

THE POLICY DIALOGUE: AN EVIDENCE-BASED POLICY DEBATE

The dialogue gathered policymakers, researchers, startups and industry experts to debate the trust architecture of European virtual worlds and regulatory sandboxes. The plenary discussion centred on three guiding questions:

- How can regulatory sandboxes be institutionalised as agile governance tools rather than bureaucratic burdens?
- What policy pathways can support cross-border, interoperable trust architectures?
- How can Europe balance openness and safety, experimentation and protection, innovation and rights?

Contributions from leading figures – among them **Emanuela Girardi, president of the AI Data Robotics Association**, **Francesco Mureddu, vice president of the Lisbon Council**, **Francesco Molinari senior research associate at the Lisbon Council** and **Arno Laeven, executive director of the European Decentralisation Institute** – set the tone for a constructive, forward-looking exchange.

THE METHODS: POLICY PROTOTYPING

2.1.1 The Policy Prototyping Design

The subsequent 90-minute co-creation workshop translated the briefs' conceptual proposals into tangible prototypes. Building on the *Policy Prototyping Design Playbook*, participants worked through two user-centred, scenario-based exercises:

- **Scenario A – The Cross-Border Worker:**
Participants explored how trust tools such as eIDAS 2.0 wallets and verifiable credentials could streamline professional certification, protect intellectual property and enhance mobility across member states.
Systemic change identified: interoperable sandboxes enabling real-time cross-border credential recognition and consent-based data sharing.
- **Scenario B – The 28th Regime as a Virtual World:**
Participants considered how immersive and decentralised technologies could underpin a European-wide virtual regime allowing entrepreneurs to establish and operate businesses beyond national borders.
Systemic change identified: sandbox pilots harmonising conflicting national regulations to create a legally certain, innovation-friendly environment for startups and micro-SMEs.

This participatory design approach anchored the recommendations in lived experience. Each scenario mapped specific user journeys and pain points to systemic reforms, turning abstract principles into

feasible, scalable solutions aligned with existing EU frameworks such as the **Digital Services Act**, **AI Act**, **eIDAS 2.0**, and the **Virtual Worlds Strategy**.

3 POLICY BRIEF 1

3.1 REGULATORY SANDBOXES FOR VIRTUAL WORLDS INNOVATION: A FRAMEWORK FOR EU LEADERSHIP

KEY TAKEAWAYS

Regulatory sandboxes are controlled environments in which innovators can test products, services, and business models under a regulator's oversight. Their goals include fostering experimentation, collecting evidence for future policymaking, and building dialogue between regulators and industry.

This OpenVerse Policy Brief explores the potential of regulatory sandboxes to offer a dynamic, adaptive, and risk-managed framework for balancing the promotion of innovation with the protection of fundamental rights in Virtual Worlds (VW). As immersive digital environments—from MetaVerse (MV) platforms to Augmented and Virtual Reality (AR/VR) applications, from Block Chain (BC) based ecosystems to Artificial Intelligence (AI) driven models and simulations—expand in complexity and societal relevance, sandboxes emerge as a crucial, and Over the past few years, the European Union (EU) has been building a coherent, future-proof framework to govern Virtual Worlds across its Member States. However, that still lacks a cohesive, VW-specific sandbox environment.

Rigid regulation can stifle progress; unregulated innovation can harm users. Sandboxes offer a third way: facilitating agile, iterative development where experimental technologies are monitored in real-time, and allowing rights enforcement to evolve alongside innovation. This doesn't come without its own complexities, which are not merely extensions of traditional Internet governance issues; rather, they are compounded by the immersive, persistent, and often decentralized nature of VW environments.

Despite the growing interest in regulating innovation in Virtual Worlds, there is a significant lack of detailed case studies around the world, matching the variety of potential, as well as actual, business applications – which range from financial to labour markets, from education to commerce, and from social interaction to public governance. If one broadens the scope to generic (i.e. not specifically oriented to VW) regulatory sandboxes, then the evidence at hand increases in quantitative terms, but the key issue remains unattended of which unavoidable characters of a sandbox environment should be associated with its utilisation for VW innovation.

Another notable gap in the public record is the absence of detailed case studies on unsuccessful sandbox projects, particularly in the MV/VW domain. While some projects may not proceed past the application stage, and others may pivot or fail within the sandbox, the reasons for these outcomes are rarely publicized. This lack of transparency makes it difficult to draw lessons from failure, which can be just as valuable as celebrating success.

Finally, this document draws the distinction between single-country and multi-country regulatory sandboxes. While the former type serves its purpose in fostering localized innovation within a single jurisdiction, the global and interconnected nature of MetaVerse and Virtual Worlds industries demands a more expansive approach, which should facilitate the temporary lifting or harmonization of complex cross-border rules, thus foster the development of systemic solutions that cut across multiple jurisdictions.

URGENCY

Over the past few years, the European Union (EU) has been building a coherent, future-proof framework to govern Virtual Worlds across its Member States. However, that still lacks a cohesive, VW-specific sandbox environment.

This Policy Brief outlines the scope and functioning of a regulatory sandboxing scheme specifically designed for new European startups and micro-enterprises operating in the MV/VW industries. The scheme is conceptualized around the principles and constitutive features of the so-called '28th Regime', an emerging legal framework aimed at fostering innovation and simplifying cross-border operations within the EU.

By institutionalizing sandboxes as a governance tool, the EU can navigate the complexities of Virtual Worlds with foresight and flexibility. Through harmonized action, stakeholder engagement, and global leadership, Europe can help ensure that the digital future remains not only innovative—but fair, inclusive, and democratic.

However, it is necessary to act swiftly to shape the normative and regulatory frameworks that will govern Virtual Worlds. Global competitors are already setting de facto standards. Delayed action risks diminishing the EU's digital sovereignty, innovation leadership, and influence in global tech governance.

Recommendations provided in this Policy Brief include fostering cross-border collaboration, establishing clear guidelines for sandbox participation, and integrating lessons learned into broader regulatory frameworks.

EXPECTED READERSHIP

Interested readers of this Policy Brief include EU, national and regional/urban policymakers and legislators/regulators, MV/VW industry stakeholders, investors and the financial community, standardisation experts, researchers, academics and advisors, legal practitioners and IT consultants, civil society and user-rights activists.

3.2 INTRODUCTION: THE PROMISE AND PERIL OF VIRTUAL WORLDS

Virtual Worlds (VW) encompass immersive digital environments that include elements of the MetaVerse (MV), Augmented and Virtual Reality (AR/VR), Block Chain (BC) based ecosystems, and Artificial Intelligence (AI) enabled interactions. These environments are reshaping the financial markets (Cantú et al., 2024), the labour markets (Greening & Fletcher, 2013), education (Crogman et al., 2025), commerce (Buzzell et al., 2023), social interaction (Hennig-Thurau et al., 2023) and public governance (Di Porto et al., 2024).

As these technologies evolve, the EU is positioned uniquely between its digital sovereignty ambitions and its strong human rights foundation. This dual mandate creates both an opportunity and a challenge: to catalyse innovation while upholding citizen rights, data protection, and democratic values.

This Policy Brief outlines the scope and functioning of a regulatory sandboxing scheme specifically designed for new European startups and micro-enterprises operating in the MV/VW industries. The scheme is conceptualized around the principles and constitutive features of the

so-called '28th Regime', an emerging legal framework aimed at fostering innovation and simplifying cross-border operations within the EU.

The structure of this document is as follows:

- Section 2 defines regulatory sandboxes, as distinct from other regulatory mechanisms – such as safe harbours and informal guidelines – and other non-regulatory sandboxes, such as controlled experimental settings and software environments. Then it outlines four key areas of concern that are peculiar to Virtual Worlds: data governance, interoperability, cybersecurity, and GDPR compliance. Finally, it makes the case and outlines the expected benefits from the adoption of regulatory sandboxes to support testing and validation of innovative MV/VW solutions.
- Section 3 summarizes the evidence gathered from a collection of European and international case studies presented in Appendix E to this document. Globally there is a notable lack of examples in the state of the art, including of unsuccessful sandbox projects, particularly in the MV/VW domain. If one broadens the scope to generic (i.e. not specifically oriented to VW) regulatory sandboxes, then the evidence at hand increases in quantitative terms, but the key issue remains unattended of which unavoidable characters of a sandbox environment should be associated with its utilisation for MV/VW innovation. The section draws a distinction between single-country and multi-country regulatory sandboxes. While the former type serves its purpose in fostering localized innovation within a single jurisdiction, the global and interconnected nature of MV and VW industries demands a more expansive approach, which should facilitate the temporary lifting or harmonization of complex cross-border rules, thus foster the development of systemic solutions that cut across multiple jurisdictions.
- Section 4 outlines the foundational principles, stakeholders, governance models, and practical guidelines required to build effective and ethical sandboxes for VW technologies. It also makes the case for the creation of a regulatory sandbox structured according to the principles of the '28th Regime'. This would create a voluntary, pan-European testing ground for startups and micro-enterprises, allowing them to innovate across borders under a single, harmonized set of rules.
- Finally, Section 5 synthesizes the strategic path forward for the European Union, offering concrete recommendations for action at both the supranational (EU) and Member State levels. Recommendations include fostering cross-border collaboration, establishing clear guidelines for sandbox participation and integrating lessons learned into broader regulatory frameworks.

Apart from the aforementioned Appendix E, the following are also attached to this Policy Brief: Appendix A is a Glossary of used terms, Appendix B is a comparative table of EU vs global jurisdictions, Appendix C describes the methodology through which the case studies gathered in Appendix E have been identified, Appendix D summarises the European state of the art and Appendix F displays the interview script used to approach the 10 international experts who have validated the initial findings presented in an earlier version of this document. Appendix G is a collection of the most significant quotes from the expert interviews.

3.3 THE REGULATORY CHALLENGE: SANDBOXES AS CATALYSTS FOR RESPONSIBLE INNOVATION IN THE EUROPEAN METAVERSE

The term ‘sandbox’ does not inherently require a regulatory body’s involvement or institutional innovation. In many domains, it simply refers to a controlled, isolated environment, where new technologies, products, software, or processes can be developed, tested, and refined, without impacting the operational functioning of ‘live’ systems. Non-regulatory sandboxes are created by organisations (private or public), typically for R&D, technical validation, or product testing, with no formal involvement or supervision from a regulatory body. In the remaining part of this section and document, we will focus on regulatory sandboxes, being overseen by a regulator and involving temporary exemptions or adjustments to regulations with a view to facilitate technological innovation. Regulatory sandboxes are not the only possible example of regulatory environments: for instance, ‘safe harbours’ offer legal protection from liability for entities complying with specific set rules or standards and provide immunity for compliant actions, but do not require testing or regulator-monitored experimentation. In turn, ‘technological free zones’ consist of geographically located physical environments, in real or near-real settings, used for testing and experimenting with direct and continuous monitoring by national regulatory authorities and other competent entities.

3.3.1 Principles and Objectives of Regulatory Sandboxes

Regulatory sandboxes are structured testing environments established by regulatory authorities that allow innovators to trial new products, services, or business models under real-world conditions, but within a controlled and supervised framework. These environments are particularly valuable in rapidly evolving sectors such as financial services (Levy-Basse & Fang, 2022), healthcare (Mathews et al., 2023), or virtual economies (Trentini, 2020), where traditional regulatory systems may lag behind technological advancement. Sandboxes operate with defined boundaries, including clear eligibility criteria, time limits, and built-in safeguards to manage risk. Their primary aim is to strike a balance between encouraging innovation and ensuring consumer protection and financial or systemic stability.

One of the central objectives of regulatory sandboxes is to encourage early-stage experimentation without exposing the broader market or public to untested risks. Innovators can test novel ideas—such as decentralized finance platforms, AI-powered diagnostics, or VW commerce applications—without immediately being subject to full regulatory requirements. Instead, they operate in a monitored environment where the impact of their products can be evaluated in real time. This approach reduces the time and cost associated with full regulatory compliance during the initial stages of innovation while still maintaining safeguards through limited scale, restricted user groups, and ongoing supervision. It does not only accelerate the development cycle but also enables regulators, who may otherwise lack firsthand exposure to such developments, to assess the potential benefits and risks of emerging technologies before they reach mass adoption (Zetzsche et al., 2017).

In addition to promoting innovation and facilitating understanding of potential risks embedded into it, regulatory sandboxes can serve as valuable instruments for evidence-based policymaking. By observing how new technologies function in practice, and especially how they behave under real-world conditions, regulators can collect empirical data to better understand potential regulatory gaps and unintended consequences. This evidence supports the development of more adaptive, flexible and relevant regulations, which is especially critical in areas where traditional rules may stifle beneficial innovation or fail to address novel risks. As noted by the Financial Conduct Authority (FCA), the UK’s sandbox has helped regulators identify where existing rules may need refinement or where entirely new frameworks are warranted to support responsible innovation (FCA, 2017).

Finally, regulatory sandboxes enhance dialogue and collaboration between regulators, industry stakeholders, and sometimes end users. This interaction builds trust and mutual understanding, supports knowledge transfer, and increases the transparency of regulatory processes. Through this engagement, innovators gain clarity on compliance expectations, while regulators stay abreast of industry trends and evolving technologies. Ultimately, regulatory sandboxes contribute to a more responsive and resilient regulatory ecosystem that promotes sustainable innovation aligned with public interest and trust (Korinek, 2023).

3.3.2 Unique Complexities of Virtual Worlds

As Virtual Worlds become increasingly integrated into sectors like finance, healthcare, and commerce, they introduce a suite of complex regulatory, ethical, and technical challenges. These complexities are not merely extensions of traditional Internet governance issues; rather, they are compounded by the immersive, persistent, and often decentralized nature of these environments.

Four key areas of concern include data governance, interoperability, cybersecurity, and legal compliance, particularly in the realm of data protection like with the EU's General Data Protection Regulation (GDPR). More details are provided in the four subsections below.

3.3.2.1 Data Governance and Consent in Persistent, Immersive Spaces

Data collection in Virtual Worlds is both continuous and multidimensional. Unlike traditional web platforms, virtual environments gather behavioural, biometric, and contextual data in real time, often without users' full awareness or explicit consent. This raises fundamental concerns about transparency and informed consent. Persistent tracking of avatars' movements, eye gaze, speech patterns, and gestures challenges conventional notions of user agency and data minimization.

Furthermore, virtual spaces often involve complex social interactions where data flows are dynamic and difficult to control. For example, one user's actions—such as recording or broadcasting interactions—can implicate the data rights of others without their explicit consent. According to Madary and Metzinger (2016), immersive technologies like VR have the potential to alter self-perception and behaviour, amplifying the ethical stakes of how data is used and shared within these environments.

Compounding this challenge is the problem of persistent digital identities. Unlike cookies or session-based trackers that can be cleared, a user's presence in a Virtual World is often continuous and accumulates a longitudinal digital footprint. Efforts like the XR Safety Initiative (XRSI, 2020) aim to create frameworks for privacy and data protection in extended reality environments, but regulation remains fragmented and reactive.

3.3.2.2 Interoperability Between Platforms and Protocols

One of the ambitions of the MetaVerse and Virtual Worlds is seamless interoperability—where users can move between platforms with their identities, assets, and data intact. However, this vision is technically and commercially difficult to achieve. Most Virtual Worlds are siloed ecosystems with proprietary standards, making cross-platform compatibility rare and fraught with challenges.

Interoperability requires agreement on data schemas, identity standards, asset formats, and communication protocols. Groups like the Open MetaVerse Interoperability (<https://omigroup.org/>) are working toward shared frameworks, but the lack of incentives for

dominant platforms to enable interoperability remains a significant barrier. Without these standards, users face vendor lock-in and limited portability of digital identities and assets.

Legal complications also arise: if a virtual item is bought on one platform but used on another, who is responsible if it malfunctions or violates terms of service? Jurisdictional ambiguities become especially problematic in a globalized, platform-agnostic environment. Governments and regulators are still grappling with how to treat digital assets and interactions that span multiple, often conflicting, legal Regimes (OECD, 2025a).

3.3.2.3 Cybersecurity Risks Across Distributed Digital Ecosystems

The decentralized and distributed architecture of many Virtual Worlds introduces new vulnerabilities for cybersecurity. These environments often integrate blockchain, edge computing, and real-time communications, creating a wide and complex attack surface. In virtual economies, cyberattacks can lead not only to data breaches but also direct financial loss, identity theft, or virtual property damage.

Unlike conventional IT systems, Virtual Worlds deal with layered infrastructure—application layers (game engines), hardware layers (VR/AR devices), and network layers—all of which can be individually or collectively targeted. A notable example is the 2022 breach of Axie Infinity's Ronin Network, where attackers stole over \$600 million in crypto assets due to a compromised validator node system (Robertson & Faife, 2022).

Moreover, user behaviour within immersive environments introduces unique threats. Deep impersonation, virtual stalking, and spatial phishing (where fake virtual assets lure users into malicious interactions) are all new forms of cyber risk that require updated threat models and mitigation strategies. Regulatory frameworks, such as the US National Institute of Standards and Technology's Cyber Security Framework (NIST, 2024), are beginning to consider these new dimensions, but widespread implementation is still nascent.

3.3.2.4 Conflicts Between Innovation and GDPR Compliance

Designed to protect users' data rights, GDPR presents a critical tension with the innovation ambitions of Virtual Worlds. These environments often rely on the continuous collection of biometric, behavioural, and location data—forms of "special category" data under GDPR that require heightened protection and explicit consent. However, the dynamic and spontaneous nature of interactions in virtual spaces makes granular consent challenging to implement and enforce (Raja et al., 2025).

In practice, the right to erasure, data portability, and purpose limitation are difficult to operationalize in persistent virtual environments. For instance, if a user wishes to delete all traces of their presence in a shared Virtual World, it may be technically impossible without also affecting others' data. Research by Smith et al. (2025) highlights the limits of applying current data protection rights to decentralized, immersive ecosystems and calls for reinterpreting GDPR in light of these challenges.

While the European Data Protection Board (EDPB) hasn't issued specific guidelines or recommendations solely on Virtual Worlds, it has addressed the application of GDPR to these environments within its broader work on online services and data processing. The EDPB's general principles and guidance on data protection remain relevant and applicable to Virtual World providers.

Additionally, data controllers in Virtual Worlds may span multiple jurisdictions, complicating the identification of legal responsibility. If a platform is hosted in the U.S., utilizes a smart contract stored on an EU server, and serves users in Asia, it's unclear which entity must comply with EU regulations. As such, innovation in Virtual Worlds must proceed with careful attention to legal design, including privacy-by-design principles and proactive risk assessments.

3.3.3 The Case for Sandboxes

The tension between fostering innovation and ensuring regulatory oversight has become more pronounced with the rise of immersive technologies and Virtual Worlds. Traditional regulatory frameworks, built for linear and well-established industries, often struggle to keep pace with the rapid evolution and unique features of virtual environments. Overly rigid regulation can inhibit the development of transformative tools in education, healthcare, and finance, while a lack of oversight risks exposing users to harms such as data misuse, discrimination, or financial exploitation. Regulatory sandboxes offer a compelling “third way”: a controlled, collaborative space where innovation can be tested under real-world conditions, with oversight from regulators and input from stakeholders.

Sandboxes enable a responsive model of governance that allows rules and technologies to evolve in tandem. Within a sandbox, developers can launch experimental services under predefined conditions, regulators can observe their impacts, and both parties can adjust protocols as needed. This approach is especially beneficial in Virtual Worlds, which combine elements of multiple regulated sectors—communications, financial services, digital identity, and data protection—into a single, complex ecosystem. As highlighted by Zetzsche et al. (2017), sandboxes allow regulators to identify which existing rules apply, where gaps exist, and whether new frameworks are needed, all without stifling early innovation.

The real-time feedback loop provided by sandboxes can be particularly valuable in the context of emerging virtual economies and identity systems. For instance, if a decentralized virtual platform introduces a novel form of biometric authentication or user-owned digital property, a sandbox allows regulators to assess its implications for privacy, security, and consumer protection before widespread rollout.

Furthermore, sandboxes foster collaboration across sectors. In the case of Virtual Worlds, this means convening developers, ethicists, cybersecurity experts, economists, and policymakers to engage in proactive governance. Such cross-disciplinary interaction is essential for addressing the hybrid challenges these environments present—such as safeguarding user autonomy while enabling platform interoperability or balancing economic innovation with anti-money laundering requirements. As OECD (2025b) notes, adaptive governance mechanisms like sandboxes can help ensure that digital ecosystems grow in a way that aligns with societal values and legal norms.

In sum, regulatory sandboxes provide a flexible, scalable solution to the policy challenges posed by Virtual Worlds. By embedding experimentation within a structured legal framework, sandboxes allow for iterative governance—enabling innovation without abdicating responsibility. Their adoption should be seen not as an exception, but as an essential component of any forward-looking regulatory strategy in the MetaVerse and beyond.

3.3.4 Expected Benefits

To summarise, the adoption of regulatory sandboxes in real-world experimentation carried out in VW environments might bring the following benefits.

3.3.4.1 Evidence-Based Policy Design

Regulatory sandboxes allow policymakers to observe emerging technologies in action, providing real-world data that can inform the development of nuanced and proportionate regulation. In the context of Virtual Worlds—where technologies such as biometric tracking, decentralized economies, and immersive interfaces are rapidly evolving—this evidence-based approach is critical. By studying how these innovations function in practice, regulators can assess their societal impacts, identify unintended consequences, and tailor legal frameworks accordingly. This proactive method reduces reliance on hypothetical scenarios and fosters more effective, targeted policies (Zetsche et al., 2017).

3.3.4.2 Multi-Stakeholder Collaboration

Sandboxes create a platform for dialogue between innovators, regulators, civil society, and technical experts. This collaborative model is especially important in virtual environments, which intersect with multiple domains including finance, health, education, and entertainment. Through structured sandbox initiatives, developers can receive early feedback from regulators, while public interest groups and academics can contribute ethical, social, and technical insights. Such inclusive engagement enhances trust, transparency, and alignment between innovation and public values (Korinek, 2023).

3.3.4.3 Risk Identification and Mitigation

Virtual Worlds carry significant risks—from data breaches and algorithmic bias to financial fraud and user manipulation. Regulatory sandboxes allow these risks to be identified early, before full-scale deployment. By simulating user interactions and system dynamics in a controlled environment, regulators can detect vulnerabilities and enforce mitigation strategies. This approach enhances user safety and helps developers build more resilient platforms. For example, sandbox trials can uncover compliance gaps related to GDPR or cybersecurity standards, enabling timely corrections before broader exposure.

3.3.4.4 Scalable Best Practices for EU-Wide Digital Frameworks

Insights generated through sandbox experiments can inform harmonized digital regulation across the European Union. As the EU works toward implementing broad initiatives like the Digital Services Act and the Artificial Intelligence Act, regulatory sandboxes can act as testbeds for scalable, interoperable governance models. The lessons learned from national sandbox projects—such as those described in the following Section of this document—can be synthesised to guide cohesive, cross-border standards for VW platforms. This supports both innovation and legal certainty and contributes to reinforce the EU's global leadership in digital rulemaking.

3.4 NAVIGATING THE COMPLEXITIES: EXAMPLES OF (IN)EFFECTIVE INTERPLAYS BETWEEN VIRTUAL WORLDS AND THE REGULATORY FRONTIER

Virtual Worlds present novel intersections of law, technology, and society—often challenging existing regulatory frameworks. This section explores how individual governments are responding through sandbox initiatives, in Europe and overseas. A more detailed presentation of the case studies used as background can be retrieved in Appendix E to this document. While

some jurisdictions have embraced agile experimentation, others remain tentative, reflecting broader tensions between innovation and control, openness and safety, or local values and global networks.

3.4.1 International Case Studies

Singapore's MAS Fintech Sandbox (NE1), the UAE's ADGM RegLab (NE3), Canada's CSA Innovation Hub (NE4), and Australia's ASIC Enhanced Sandbox (NE5) exemplify **financial innovation-oriented models**. These frameworks prioritize Block Chain, digital assets, and AI-driven financial services, providing temporary regulatory relief to test novel business models. While not explicitly VW-focused, they establish essential infrastructure for virtual economies—digital payments, tokenization, and decentralized finance (DeFi)—that underpin MetaVerse transactions. Singapore's success in attracting 630+ FinTech applications demonstrates how such sandboxes can catalyse ecosystem growth while informing iterative regulatory refinements.

Singapore's Virtual Singapore (NE2) and China's state-directed NFT/blockchain initiatives (NE8) represent **spatial-digital hybrid approaches**. Virtual Singapore—a SGD 73 million 3D city twin—functions as a technical sandbox for simulating urban planning and disaster response, leveraging VR interfaces and IoT integration. China's strategy, though constrained by anti-speculation policies, invests €600+ million in "practical MetaVerse" applications (e.g., digital tourism, education). Both highlight how digital twins bridge physical governance and virtual experimentation, though China's model prioritizes state control over open innovation.

Japan's Cabinet-Level AR/VR Sandbox (NE7) and the U.S. FDA Digital Health Center (NE10) adopt **verticalized regulatory pathways**. Japan's permanent sandbox enables cross-ministerial testing of AR/VR in healthcare, mobility, and manufacturing, leading to 30+ approved projects and evidence-based regulatory reforms. The U.S. FDA's framework, while not a formal sandbox, operates analogously — streamlining approvals for VR medical devices (e.g., PTSD therapy, surgical training) via pre-submission guidance and expedited reviews. These cases underscore how targeted regulatory agility fosters high-impact VW applications in critical sectors.

South Korea's MetaVerse Industry Promotion Act (NE9) transcends sandbox logic entirely, establishing the world's first comprehensive **VW governance framework**. Backed by \$186 million in state funding, it integrates VR/AR development, digital identity standards, and ethical guidelines while enabling industry self-regulation. This legislative approach—complemented by AR/VR intellectual property protections—positions South Korea as a pioneer in systemic VW advancement, contrasting sharply with fragmented, sector-specific sandboxes elsewhere.

These international cases reveal sandboxes as **policy laboratories** where States negotiate innovation imperatives against regulatory stability. While FinTech-oriented models dominate, emergent frameworks for AR/VR (Japan), medical VW (USA), and national MetaVerses (South Korea) signal a paradigm shift toward immersive digital governance. Yet the absence of cohesive transnational sandboxes remains a barrier to seamless Virtual World integration—a challenge demanding innovative multilateral solutions.

3.4.2 European Case Studies

In Europe, some Member States and Associated Countries have piloted their own regulatory sandboxes to explore the boundaries of immersive digital technologies.

The United Kingdom's MHRA Digital Health Sandbox (E1) exemplifies sector-specific regulatory agility. By granting Oxford VR temporary exemptions from medical device certification, it accelerated the clinical validation of VR-based cognitive behavioural therapy,

culminating in CE marking and NHS adoption. Similarly, France's CNIL-led pilots in education (E3) and healthcare (E4)—despite discontinuation risks—demonstrated how temporary GDPR waivers enabled real-world testing of VR classrooms and medical simulators. Nordic innovations extended this further: Norway's AI/VR Labour Sandbox (E12) refined data governance for virtual job interviews, while Finland's TEKIA project (E13) achieved a 34% job placement rate using Unreal Engine-based VW assessments under derogated counselling rules. These cases underscore **sandboxes as catalysts for high-impact social applications**, though scalability remains constrained by national borders.

The European Block Chain Sandbox initiative represents the EU's most advanced transnational regulatory experiment. Cases like Circularise's supply-chain traceability platform (E6, Netherlands), DigiShares' real estate tokenization (E11, Denmark), DoxyChain's digital credentials (E15, Poland), and Konnecta's secure communications (E19, Greece) reveal a shared methodology: multi-regulator dialogues testing solutions against harmonized frameworks (eIDAS, GDPR, MiCA). The EBS's focus on interoperability and digital identity—exemplified by OriginTrail's decentralized knowledge graphs (E16, Slovenia)—directly enables future VW infrastructures. This model uniquely addresses fragmentation by providing a **"single entry point" for pan-European compliance validation**.

Germany's Reallabore-Gesetz (E7) established a permanent regulatory testbed framework, enabling sectoral diversity from mobility to manufacturing. Its sub-projects highlight VW integration: ARENA2036's industrial MetaVerse (E8) blends VR/AR with physical production under waived safety regulations, while Hamburg's digital twin (E9) uses participatory VR urban planning to circumvent GDPR barriers. Ahaus' commerce platform (E10)—operational since 1986—demonstrates longevity in blending physical/digital economies. These cases illustrate how **national legislation can institutionalize sandboxes**, though cross-sector replication remains uneven.

Most national approaches reveal **persistent fragmentation**. Spain's AI-focused financial sandbox (E18) and Italy's Sperimentazione Italia (E17) prioritize sectoral innovation but lack VW-specific mechanisms. The Netherlands' PETs sandbox (E5) advances privacy-enhancing technologies yet remains domestically bounded. Portugal's Technological Free Zones (E20) offer geographic flexibility for immersive tech testing but produced limited scalable outcomes. Only the UK's FCA "Supercharged Sandbox" (E2)—partnering with NVIDIA—explicitly incorporated VR/AR financial applications, signalling awareness of converging technologies.

Although these efforts differ in scope and focus, they collectively illustrate how some national governments are leveraging experimental legal spaces to explore Virtual Worlds' complex intersections with data protection, digital sovereignty, and platform regulation. They also highlight the importance of **maintaining coherence with overarching EU digital strategies**, such as the Virtual Worlds Initiative and the Artificial Intelligence Act.

3.4.3 Key Comparative Insights

The comparative table in Appendix B describes in more detail the distinctive characteristics of the analysed case studies. These are noteworthy in five principal directions, as reported below.

Sectoral Breadth:

- Europe: Dominated by healthcare/fintech (60% of cases); emerging industrial VW focus in Germany.
- Global: South Korea/Japan prioritize national VW ecosystems; China/UAE emphasize state-aligned applications.

Oversight Flexibility:

- Europe: Fragmented national authorities (exceptions: BCS multi-regulator model).
- Global: Centralized tech-focused bodies (e.g., Korea's MSIT, Japan's Cabinet Secretariat).

Data Rights Adaptation:

- Europe: Relies on GDPR waivers; limited innovation beyond compliance.
- Global: Korea/Japan implement VW-specific ethical frameworks; USA enforces medical safety standards.

Innovation Scale:

- Europe: Germany's legislative permanence contrasts with France/Italy's pilot discontinuation.
- Global: Singapore/South Korea combine funding (\$186M–SGD 73M) with regulatory agility.

5. VW Strategic Alignment:

- Europe: EBS focuses on blockchain infrastructure; lacks immersive tech prioritization.
- Global: Korea/Japan legislate VW governance; China enforces state-controlled digital twins.

3.4.4 From Sandboxing to Regulation

The examples provided highlight the importance of coherent institutional support, multi-agency collaboration, and regulatory foresight. However, they also illustrate ongoing struggles—such as how to align real-time innovation with slower-moving legal systems and ensure that sandbox findings are translated into scalable policy.

A critical next step for sandboxed innovation is transitioning from isolated pilot programs to integrated regulatory and competitiveness strategies. Successful experiments can provide a foundation for broader legal reforms, public-private partnerships, and digital economy investments. For example, insights from sandboxes on digital identity management can inform future regulations on cross-border e-ID interoperability, while trials involving tokenized assets in Virtual Worlds may shape digital euro frameworks or crypto asset legislation.

To make this transition prompter, EU Member States should invest in knowledge translation mechanisms—such as policy briefs, white papers, and inter-agency task forces—that can distil technical findings into actionable guidelines. The European Commission has already indicated its support for "regulatory learning by doing" models through initiatives like the EU Digital Decade and its Artificial Intelligence Pact. However, to be successful, these mechanisms should harmonize local policy innovation with continental strategies, reinforcing Europe's digital sovereignty and competitiveness.

Moreover, sandboxes should act as testing grounds not only for technologies but for regulatory approaches themselves, such as risk-based supervision, real-time monitoring, or co-regulatory Regimes. The challenge lies in avoiding siloed outcomes and ensuring that lessons learned inform adaptable, sector-agnostic governance tools.

3.4.5 Risks and Mitigations

Despite their promise, regulatory sandboxes carry inherent risks. One major concern is regulatory capture, where large or influential firms may gain disproportionate access to policy influence through sandbox participation. If not designed equitably, sandboxes can also exclude smaller innovators, civil society groups, or underrepresented stakeholders, thereby entrenching existing power asymmetries. Additionally, there's the danger of "sandbox inertia", where regulatory reform is indefinitely postponed in favour of endless pilot programs without systemic change.

To address these risks, sandbox governance must emphasize transparency, inclusivity, and accountability. Clear entry criteria, public reporting requirements, and the involvement of independent advisory boards can help ensure balanced stakeholder representation. Furthermore, funding support for smaller or mission-driven participants can democratize access to experimental governance opportunities.

Another risk lies in undermining fair competition. Sandboxes must be carefully calibrated to promote innovation without granting *de facto* regulatory exemptions that distort markets. As immersive platforms increasingly monetize attention, labour, and assets within Virtual Worlds, regulators must ensure that sandbox benefits are not monopolized by dominant platforms or used to delay necessary structural reforms.

Balancing innovation with market integrity requires ongoing monitoring, strong institutional safeguards, and a willingness to sunset sandbox privileges once risks are fully understood. Done well, regulatory sandboxes can become foundational tools for 21st-century digital governance, merging experimentation with ethical and sustainable rulemaking.

3.4.6 Necessity of Specialisation

Despite the growing interest in regulating innovation in Virtual Worlds, there is a significant lack of detailed case studies around the world, matching the variety of potential, as well as actual, business applications – which range from financial to labour markets, from education to commerce, and from social interaction to public governance. If one broadens the scope to generic (i.e. not specifically oriented to VW) regulatory sandboxes, then the evidence at hand increases in quantitative terms, but the key issue remains unattended of which unavoidable characters of a sandbox environment should be associated with its utilisation for VW innovation.

Another notable gap in the public record is the absence of detailed case studies on unsuccessful sandbox projects, particularly in the MV/VW domain. While some projects may not proceed past the application stage, and others may pivot or fail within the sandbox, the reasons for these outcomes are rarely publicized. This lack of transparency makes it difficult to draw lessons from failure, which can be just as valuable as celebrating success.

Finally, we would like to draw the distinction between single-country and multi-country regulatory sandboxes. While the former type serves its purpose in fostering localized innovation within a single jurisdiction, the global and interconnected nature of MetaVerse and Virtual Worlds industries demands a more expansive approach, which should facilitate the temporary lifting or harmonization of complex cross-border rules, thus foster the development of systemic solutions that cut across multiple jurisdictions.



3.5 DESIGNING SANDBOXES FOR VIRTUAL WORLDS

The complexity and dynamism of Virtual Worlds demand a tailored approach to regulatory experimentation. As immersive environments become increasingly integrated into digital economies and social infrastructures, regulatory sandboxes must be designed with sector-specific nuances in mind. This section outlines the foundational principles, stakeholders, governance models, and practical guidelines required to build effective and ethical sandboxes for VW technologies. It also makes the case for a regulatory sandbox structured according to the principles of the so-called ‘28th Regime’. This would create a voluntary, pan-European testing ground for startups and micro-enterprises, allowing them to innovate across borders under a single, harmonized set of rules.

3.5.1 Key Pillars

Effective sandboxes for Virtual Worlds must rest on robust foundations. One of the most critical pillars is **data governance**. Virtual Worlds often involve persistent data collection experiments involving personal data—tracking biometric inputs, behavioural patterns, and real-time interactions. This raises acute concerns under the General Data Protection Regulation (GDPR), particularly around informed consent, data minimization, and the right to erasure. Sandboxes must rigorously test how immersive technologies handle **personal information** and assess compliance with both current GDPR provisions and anticipated extensions, such as those related to emotion recognition and automated decision-making.

Another foundational element is **interoperability**. Virtual ecosystems are currently siloed, with dominant platforms creating closed environments that hinder user mobility and innovation. Sandboxes should support experiments in open standards, protocol alignment, and cross-platform data portability—essential for a healthy, competitive MetaVerse. Additionally, **protection from cybersecurity threats** must be integral from the outset. Virtual worlds expand the attack surface significantly, from avatar hijacking to smart contract vulnerabilities. Sandbox testing should include stress-testing of security mechanisms in both client and server-side implementations.

Ethical AI implementation within Virtual Worlds represents another key challenge. Many of these environments rely on AI for content moderation, recommendation engines, and adaptive NPCs (non-player characters). Sandboxes offer a critical setting to evaluate bias, explainability, and accountability of these algorithms in immersive contexts. Finally, market fairness must guide sandbox design. Given the concentration of power in current virtual platform providers, sandboxes must ensure equal access to testing opportunities and actively guard against reinforcing monopolistic structures. This includes enforcing non-discriminatory terms and establishing oversight mechanisms for equitable participation.

Last, but not least important pillar is **market fairness**: access and operation of the implemented sandboxes should be set up in a way to prevent monopolistic practices and ensuring parity of treatment for all economic players, including (but not limited to) start uppers and SME owners engaged in the delivery of innovative solutions.

3.5.2 Stakeholder Engagement and Collaboration

A successful sandbox ecosystem hinges on inclusive **stakeholder collaboration**. Regulators provide legal clarity and ensure alignment with policy goals. Technology companies bring technical know-how and deploy experimental systems. Civil society actors—including digital rights groups, academia, and non-profits—play a watchdog role, offering critical ethical and social impact assessments. Perhaps most importantly, users themselves should be empowered as active stakeholders, contributing feedback on usability, safety, and inclusion.

To maintain legitimacy and impact, sandbox participation should be governed by **transparent entry and exit criteria**. These might include innovation potential, consumer protection safeguards, GDPR alignment, and technical interoperability standards. Exit mechanisms must be defined in advance: participants must either progress toward compliance, pivot based on findings, or cease operations if risks outweigh benefits. Clear criteria avoid regulatory ambiguity and prevent prolonged regulatory limbo.

Moreover, each sandbox should establish **guidelines and evaluation metrics** for participation. These may include technical benchmarks (e.g., latency thresholds, API performance), regulatory indicators (e.g., compliance readiness), and social outcomes (e.g., accessibility scores, user trust levels). Metrics must be co-developed with all stakeholders and reviewed periodically to ensure relevance. This transparency builds trust and facilitates evidence-based policymaking.

3.5.3 Governance Structures and Oversight Mechanisms

Governance for Virtual World sandboxes must accommodate the **cross-border nature of digital platforms**. Virtual Worlds operate beyond national boundaries, and their regulation must reflect this transnational reality. Therefore, sandbox frameworks should be interoperable across jurisdictions, potentially coordinated through supranational bodies like the European Commission or the Global Financial Innovation Network (GFIN). Shared data spaces and mutual recognition of testing protocols could streamline multi-country experimentation.

An essential function of sandbox governance is to **learn from experience**. This means embedding feedback loops and evaluation mechanisms into the sandbox lifecycle. Post-mortems, stakeholder debriefs, and longitudinal data analysis should be standard practice. Lessons from each cohort must be codified and disseminated to policymakers, industry, and the broader public. Governance structures should also incorporate ethics review boards or independent panels to audit outcomes and provide public accountability.

Sandbox governance must **balance agility with control**. Real-time regulatory feedback—where regulators are embedded in testing teams—can accelerate safe deployment. However, this should not substitute for broader democratic oversight. By institutionalizing transparency, structured learning, and adaptive rulemaking, sandboxes can evolve from isolated pilots into engines for sustainable governance innovation.

3.5.4 General Principles for Implementation in Virtual Environments

To translate the sandbox model into Virtual World settings, it is essential to comply with some general implementation principles.

First, **data collection, usage and transparency rules** must be clearly articulated. Participants should document what data is collected (including biometric, behavioural, and spatial data), how it is processed and stored, and how users can manage their consent. All data practices should be auditable, user-facing, and adaptable to emerging data rights frameworks, such as the EU's Data Governance Act and AI Act's high-risk categorizations. As demonstrated in Finland's TEKIÄ project (E13), granular consent protocols for behavioural data are critical for ethical VW deployment.

Second, **compliance with GDPR and its potential extensions** must be central to sandbox design. This includes not just procedural adherence but stress-testing technical systems for privacy-by-design and privacy-by-default principles to be embedded in their architectures. Sandboxes can simulate real-world pressures—like data breaches during peak user loads, user escalation, or AI misjudgement in avatar interactions—to test the robustness of data protection protocols. Special attention must be paid to high-risk scenarios, described in

healthcare VW case studies (E1, E4), such as children's use of virtual spaces or the blending of medical data with immersive wellness apps. Norway's labour-market sandbox (E12) exemplifies GDPR-aligned VR data processing.

Third, **interoperability and open standards** should be promoted to counteract fragmentation. Sandboxes should require or encourage use of open APIs, universal avatar protocols, and non-proprietary file formats. This fosters competition and allows smaller innovators to build on shared infrastructure, reducing dependency on dominant platforms and mitigating platform lock-in. By enabling cross-platform avatars or currency compatibility, sandboxes can help create a more fluid and user-centric MetaVerse. VW sandboxes should mandate open APIs, universal avatar protocols (e.g., W3C Verifiable Credentials), and non-proprietary asset formats. This enables cross-platform portability of identities, assets, and experiences – reducing dependency on walled gardens. The European Blockchain Sandbox (E6, E11, E15) proves multi-vendor interoperability is achievable under regulatory supervision.

Fourth, **mitigating fragmentation and platform lock-in** is of paramount importance. Sandboxes should enforce technical and regulatory interoperability standards across jurisdictions. This includes testing cross-border digital identity (e.g., eIDAS 2.0 wallets), universal content moderation frameworks, and compatible virtual asset rules. Germany's Reallabore (E7-E10) shows how national legislation can harmonize testing, while the EU must scale the EBS model to VWs to prevent platform-centric silos.

Fifth, **security vulnerabilities and cyber threats should be addressed** effectively. Proactive threat modelling for immersive-specific risks is essential: avatar impersonation, spatial data hijacking, VR-induced physiological harms, and smart-contract exploits. Sandboxes should simulate attacks (e.g., ransomware in industrial MetaVerses) and validate defences using frameworks like UL 8400 (adopted in US case NE10). Sweden's emergency-service VR training (E14) highlights security-critical simulations.

Lastly, **security, safety, and inclusivity** must be proactively embedded. Virtual environments can amplify both harm and benefit; sandbox tests must examine safety features like content moderation, identity verification, and harassment prevention. Accessibility should be measured not only in terms of disability compliance but also language support, bandwidth flexibility, and device inclusivity. Safety features – content moderation, identity verification, and harassment prevention – must be stress-tested with vulnerable groups. Portugal's Geographic Free Zones (E20) enabled real-world inclusivity testing, while South Korea's ethical guidelines (NE9) provide a governance blueprint. By simulating edge-case scenarios and vulnerable user journeys, sandboxes can help create Virtual Worlds that are secure, ethical, and open to all.

Adopting those principles can transform sandboxes from regulatory exemptions into structured innovation engines – proactively shaping ethical, interoperable, and secure Virtual Worlds. Failure to address the principles risks replicating Web2's fragmentation and safety failures in immersive environments.

3.5.5 An Experimental Sandbox for the “28th Regime”

A potential solution to the complex challenge of regulating the nascent MetaVerse (MV) and Virtual Worlds (VW) industry in Europe may derive from an experimental regulatory sandbox structured according to the principles of the “28th Regime”. This would create a voluntary, pan-European testing ground for startups and micro-enterprises, allowing them to innovate across borders under a single, harmonized set of rules.

Such a scheme would be a significant departure from the current fragmented landscape. While the EU is actively promoting sandboxes for AI and has a European Blockchain Sandbox, these are primarily national or topic-specific initiatives. A “28th Regime Sandbox” for the MV/VW

would offer a truly unified framework, accelerating innovation while providing legal certainty for the most agile and often most vulnerable market players.

3.5.5.1 The "28th Regime" Principle: A Foundation for Borderless Sandboxes

The concept of a "28th Regime" is a proposed optional legal framework that operates alongside the 27 national legal systems of the EU Member States. Its core tenets are:

- **Voluntary Opt-In:** companies are not forced to use it. They can choose to be governed by this single set of EU rules for specific activities, or they can remain under their national legal system.
- **Harmonization and Uniformity:** it replaces a patchwork of 27 different national laws with one common, predictable legal code.
- **Reduced Compliance Costs:** businesses, especially startups, can save significant time and money by not having to navigate the legal complexities of each individual Member State they wish to operate in.
- **Single Market Enabler:** it is designed to overcome legal fragmentation, a key barrier to a truly integrated Single Market.

Applying these principles to a regulatory sandbox creates a powerful tool for fostering a competitive European MetaVerse industry.

3.5.5.2 Scope of the "28th Regime" Regulatory Sandbox

The scope of this hypothetical sandbox should be carefully defined to maximize its impact while ensuring robust oversight.

1. Eligible Participants

The sandbox would be exclusively open to startups and micro-enterprises (as defined by the EU) that are legally established within a Member State. This focus ensures that the scheme benefits those who face the highest barriers to entry and cross-border scaling due to compliance costs.

2. Eligible Innovations

Participants would need to propose a genuinely innovative product, service, or business model within the MV/VW industry. This could include, but is not limited to:

- **Novel Social Platforms:** Virtual Worlds with new forms of user interaction, content creation, and governance.
- **Economic Models:** systems involving the creation, sale, and exchange of virtual assets, digital goods, and virtual currencies.
- **Identity and Avatar Technologies:** new approaches to user identity, data ownership, and interoperability of avatars across different platforms.
- **Immersive Commerce and Experiences:** innovative retail, entertainment, education, or work collaboration models in a virtual environment.

3. The "Opt-In" Agreement

Upon acceptance into the sandbox, the startup should voluntarily agree to operate exclusively under the "28th Regime Sandbox" rules for the duration of the testing period. This single set of rules would temporarily supersede specific, pre-identified national regulations in participating Member States that pose a barrier to the innovation.

4. Pan-European Legal Passport

The key feature of the Sandbox scope should be that participation grants a “legal passport” to test the innovation with real consumers across all participating EU countries, without needing separate approvals from each national regulator.

3.5.5.3 Functioning of the "28th Regime" Sandbox

The functioning of the sandbox would be designed for clarity, efficiency, and safety, involving a clear lifecycle for participating startups.

Phase 1: Application and Admission

Distinctive features of this phase would be the following:

- **Single Point of Entry:** startups would apply through a centralized EU portal, likely managed by a new "European MetaVerse and Virtual Worlds Board" or an existing body like the European Innovation Council.
- **Harmonized Criteria:** admission would be based on a clear set of criteria, including the innovativeness of the project, its potential contribution to the EU digital single market, the identification of specific legal uncertainties to be tested, and a robust plan for consumer protection and risk mitigation.
- **Duration:** a startup would be granted entry for a fixed period, typically 12 to 24 months.

Phase 2: Experimentation and Testing

In accordance with the general principles and key pillars discussed earlier, distinctive features of this phase would be the following:

- **The Single Rulebook:** the startup should operate under a harmonized "Sandbox Rulebook". This rulebook would provide a clear legal framework on key issues plaguing the VW industry, such as:
 - **Data Protection:** a unified interpretation of GDPR principles for avatar data, biometric information, and user interaction logs.
 - **Consumer Rights:** clear rules on in-world purchases, the nature of virtual assets (goods vs. services), and dispute resolution.
 - **Content Moderation:** a baseline for defining and handling illegal vs. harmful content, aligned with the Digital Services Act (DSA) but adapted for immersive environments.
 - **Liability:** a clear framework for determining liability between platform owners, content creators, and users.
- **Unified Supervision:** would be conducted by a “Lead Supervisory Authority”, likely the national regulator of the country where the startup is based, working in close cooperation with the "European MetaVerse and Virtual Worlds Board" and other relevant national authorities. This "one-stop-shop" for supervision is a core principle of the 28th Regime.
- **Safeguards:** strict consumer safeguards would be mandatory, including informed consent from users, clear disclosure that they are participating in a test, limits on user numbers or transaction volumes, and a clear and accessible process for complaints and redress.

Phase 3: Exit and Evaluation

Distinctive features of this phase would be the following:

- **Final Report:** at the end of the sandbox period, the startup must submit a detailed report on its findings, including data on performance, risks encountered, and consumer feedback.
- **Regulatory Learning:** the supervisory authorities and the "European MetaVerse and Virtual Worlds Board" should analyse the results to draw lessons for future regulation. This "regulatory learning" is a primary goal of the sandbox.
- **Transition Path:** upon successful completion, there would be several potential outcomes:
 - **Market Authorization:** if the innovation is found to be compliant with existing EU law, it would receive authorization to be rolled out across the EU.
 - **Path to Compliance:** if minor adjustments are needed, the regulators would provide a clear roadmap for the startup to achieve full compliance.
 - **Evidence for Law Reform:** if the innovation proves beneficial but is fundamentally incompatible with current laws, the results would serve as powerful, evidence-based input for the European Commission and Parliament to amend existing legislation or propose new, innovation-friendly regulations.

By combining the agility of a regulatory sandbox with the scale and simplicity of a 28th Regime, the EU could create a uniquely powerful incubator for its next generation of digital pioneers from the European MV/VW industry. It would be a clear statement of intent to lead not only in regulation but also in fostering homegrown innovation for the Virtual Worlds of tomorrow.

3.6 CONCLUSIONS AND RECOMMENDATIONS

The rapid expansion of Virtual Worlds presents both a significant opportunity and a profound regulatory challenge. As these environments become central to digital economies, social life, and innovation ecosystems, regulators must ensure that legal frameworks remain agile, inclusive, and anticipatory. Regulatory sandboxes offer a promising mechanism to balance innovation with oversight, allowing for real-time learning, risk mitigation, and collaborative governance. This final section synthesizes the strategic path forward for the European Union, offering concrete recommendations for action at both the supranational and Member State levels.

3.6.1 Developing a Harmonized EU Framework for Sandboxes

To fully leverage the benefits of sandboxes in Virtual World governance, the European Commission (EC) and EU Member States should co-develop a harmonized regulatory sandbox framework. This would serve as a common blueprint to guide national efforts, ensure regulatory consistency, and reduce compliance fragmentation. Such a framework should align with existing digital legislation—especially the Digital Services Act, the Digital Markets Act, the AI Act, and the GDPR—while also anticipating gaps specific to immersive, persistent environments.

The EC should spearhead the creation of a cross-border sandbox infrastructure through coordination platforms, interoperability standards, and shared evaluation methodologies. This could be modelled on existing EU sandbox pilots, such as the European Block Chain Sandbox and the upcoming AI sandboxes under the AI Act. Member States, in turn, should be encouraged (and funded) to adopt sandbox-friendly legislation—like Germany’s Reallabore Act—and designate responsible supervisory authorities that collaborate across sectors (e.g., data protection, consumer rights, competition, and digital innovation).

Crucially, the harmonized framework should include mechanisms for knowledge exchange and mutual recognition. Lessons learned in Finland or France, for example, should inform ongoing experiments in the same domain run elsewhere. A central EU Sandbox Observatory should collect, evaluate, and disseminate findings, facilitating iterative policy design and ensuring best practices are shared across the Union.

3.6.2 Positioning the EU at the Forefront of Open Virtual Worlds Governance

The EU has a strategic opportunity to lead the global governance of open and ethical Virtual Worlds. While other jurisdictions—such as Singapore, the UK, and the United States—are advancing in sector-specific sandbox innovation, the EU stands out for its integrated digital policy landscape, strong commitment to human rights, and emphasis on market fairness. This positions it to champion an alternative model of immersive innovation that prioritizes trust, inclusivity, and public accountability.

China has made substantial progress in its MetaVerse development, attracting significant investment and integrating VR/AR into key sectors. However, the success is measured within a highly controlled regulatory environment that prioritizes stability and state control over market liberalization, particularly concerning the financial aspects of NFTs and cryptocurrencies.

South Korea has taken a pioneering role in fostering the MV industry with the enactment of the Metaverse Industry Promotion Act. This legislation aims to establish a comprehensive regulatory framework for VR/AR technologies, digital identity systems, and VW governance to foster systematic industry development. The purpose is to promote the growth of the

MetaVerse sector, support related companies, create jobs, and establish ethical guidelines for its development and use.

By embedding democratic values into the governance of virtual environments, the EU can push back against monopolistic, opaque, or extractive approaches to the MV/VW and related technologies. Regulatory sandboxes provide a key vehicle to demonstrate how experimentation and rights protection can coexist. Pilot programs within the sandbox framework can test practical approaches to GDPR compliance, algorithmic transparency, and AI fairness in immersive settings—offering a counterpoint to "move fast and break things" models prevalent in other markets.

The EU should also use its regulatory influence—particularly in trade, data protection, and digital standards—to shape international norms around Virtual World governance. Sandboxes offer a practical arena to pilot not just technical solutions, but institutional arrangements for transatlantic and multilateral collaboration. Through leadership in sandbox innovation, the EU can help define what a safe, interoperable, and open MetaVerse looks like on the global stage.

3.6.3 Towards a Trustworthy, Secure, and Innovative OpenVerse

Looking ahead, the EU must take bold, coordinated steps to foster a trustworthy and secure "OpenVerse"—an interconnected, user-centric MetaVerse rooted in European values. This requires more than policy declarations; it demands concrete investments in pilot programs, public-private partnerships, and long-term research. EU institutions should launch a dedicated "Virtual Worlds Sandbox Accelerator" under Horizon Europe or the Digital Europe Programme, supporting experiments across key sectors: education, finance, public services, healthcare, and culture.

Funding should be allocated not only for technological development but also for ethical testing, user experience research, and cross-disciplinary collaboration. Legal innovation is just as critical as technical progress. Sandboxes should be used to explore questions of legal identity, AI explainability, and digital labour protections—issues central to the future social contract of immersive technologies.

Finally, the EU must foster international partnerships to prevent fragmentation of the Virtual World ecosystem. This includes aligning sandbox efforts with likeminded jurisdictions (e.g., Canada, Japan, New Zealand), working with international standards bodies (e.g., ISO, IEEE), and promoting common protocols through the WTO and OECD. The OpenVerse must be pluralistic, secure, and interoperable, qualities that only collective governance, grounded in transparency and experimentation, can ensure.

3.6.4 The Imperative of the "28th Regime" and the OpenVerse Crucible

The recent Letta Report (April 2024) provides a crucial conceptual leap: the "Digital Single Market 2.0" requires a "28th Regime" – a harmonised EU legal framework operating alongside national rules, specifically designed to enable seamless scaling for startups. The emerging European OpenVerse initiative is the perfect vessel to instantiate this for Virtual Worlds.

To that end, the EU should rapidly operationalise the OpenVerse not just as a technical platform, but as the regulatory and operational scaffold for this new Regime. The "28th Regime sandbox" should become the primary entry point and testing ground for pan-European VW projects, providing a unified legal environment and technical standards, directly enabling the scale currently stifled by fragmentation.

Future sandboxes, especially for AI and VW under the OpenVerse/"28th Regime," must aggressively prioritise thematic diversity. Recruitment must target industrial simulation, immersive education, telehealth, public service delivery, cultural heritage preservation, and green innovation. The EC should consciously move beyond the financial sector's dominance in many existing models, fostering applications that deliver tangible societal and economic value across the breadth of European life.

A cross-border approach is non-negotiable for the future. AI and VW sandboxes under the European OpenVerse umbrella must be inherently multi-country. They must focus on experiments that only make sense across borders, testing interoperability, mutual recognition (especially of e-Identity), data portability, and compliance with the core pillars of the EU's digital rulebook (DSA, DMA, Data Act, AI Act). This is where true European value is created and where global competitors cannot easily replicate our unique single market advantage.

The ultimate goal is the emergence of vibrant, pan-European startups leading in VW domains. The "28th Regime" via the OpenVerse, coupled with dedicated support mechanisms – simplified cross-border sandbox access, targeted EIC Accelerator funding tailored for VW scale-up, and leveraging public procurement for innovative EU solutions – can create the fertile ground where these champions can take root and thrive from day one, thinking European scale.

4 POLICY BRIEF 2

4.1 TRUST TOOLS FOR IMMERSIVE TECHNOLOGIES

Europe is on the cusp of an epochal shift. The evolution toward Web 4.0 and immersive technology societies marks the first time that the digital, physical and virtual dimensions of human experience are converging into a single continuum. This transformation is not only technological but also social, economic, political and cultural. It reshapes how citizens learn, work, govern themselves, and relate to one another. The stakes are high: immersive technologies can either deepen trust in European institutions, markets and communities, or it can undermine it by amplifying surveillance, exclusion and manipulation.

Trust is the missing layer of the digital age. For decades, the internet has been built around principles of connectivity, speed and openness, but not around systematic trust. The last generation of digital platforms -Web 2.0 social networks, app ecosystems and data-driven services- demonstrated what happens when trust is left as an afterthought: scandals around privacy violations, disinformation, algorithmic bias and platform manipulation. These challenges have eroded public confidence in digital environments. In the emerging era of immersive, persistent and interoperable virtual worlds, the costs of neglecting trust will multiply. Unlike Web 2.0, where interactions remained largely screen-based, Web 4.0 environments will monitor movements, gestures, biometrics, and even neurological signals. Without robust trust frameworks, the risk of abuse becomes systemic.

The European Union is uniquely positioned to take the lead. Its regulatory foundations—GDPR, eIDAS, the Digital Services Act (DSA), and the Markets in Crypto-Assets Regulation (MiCA)—already provide the most comprehensive global framework for human-centric digital governance. These instruments can serve as building blocks for a new generation of “trust tools” that operationalise Europe’s values in immersive technologies. Moreover, the EU has an established reputation as a global standard-setter. Just as the GDPR became the de facto template for data protection worldwide, Europe now has an opportunity to define what trust means in the 21st-century internet.

This policy brief proposes a comprehensive “Trust by Design” framework for Europe. It draws from three major sources of evidence:

- OPENVERSE Stakeholder Consultations (Deliverables D3.1–D3.5): which captured the perspectives of SMEs, citizens, policy experts, and industry stakeholders on governance, identity, inclusivity and trust.
- EU Blockchain Observatory and Forum (EUBOF) Report: which assessed blockchain-enabled virtual worlds and offered a PESTLE (political, economic, social, technological, legal, environmental) analysis of open vs. closed approaches.
- Global Multistakeholder Conference on Web 4.0 (2025): which underscored the importance of embedding openness, interoperability and human rights into the next phase of the internet.

Key findings from these inputs include:

- There is strong consensus that interoperable identity frameworks and verifiable credentials are critical enablers of trust across platforms.
- Blockchain-based solutions—such as Decentralised Autonomous Organisations (DAOs), Non-Fungible Tokens (NFTs) and smart contracts—can underpin decentralised governance, ownership and accountability in virtual worlds.
- Stakeholders emphasised the importance of participatory governance methods, inclusivity benchmarks (such as WCAG accessibility standards) and ethical safeguards (such as audit trails for AI-driven decisions).
- Europe’s legal frameworks already contain latent trust mechanisms (consent, transparency, accountability, identity verification), but they must be adapted for immersive, persistent and decentralised environments.
- Without intervention, the risk of fragmentation into closed ecosystems -dominated by a handful of corporate actors- remains high, undermining interoperability and democratic control.

The Executive Summary highlights three core recommendations:

1. Adopt an EU Trust by Design Framework: a cross-sectoral approach embedding privacy, inclusivity, interoperability and accountability into the technical and regulatory architecture of Web 4.0.
2. Launch EU Trust Tools Sandboxes: experimental environments under the 28th regime principle, enabling cross-border testing of trust tools (identity, consent, AI audit trails) without the burden of fragmented national rules.
3. Create a European Trust Label: a certification mechanism for platforms and organisations that adhere to EU trust standards, signalling reliability and accountability to citizens and businesses.

By implementing these measures, the EU can ensure that immersive technologies strengthen rather than erode trust. It can demonstrate that immersive digital innovation is compatible with sovereignty, inclusivity and human dignity. And it can provide the global benchmark for the governance of Web 4.0, much as it has done in previous digital transitions.

Prelude: in a not so distant future

Mira’s phone buzzed as she stepped out of the co-working space into the cool Brussels afternoon. She tucked it into her coat pocket without looking. She didn’t need to — her wallet, keys, ID, and work credentials were already stitched into her decentralised identity. No more juggling logins or scanning QR codes. She just was.

At the corner café, she greeted the owner, Malik, with a warm smile. “Café noir, s’il te plaît.” He tapped a button on the café’s tablet, and Mira’s DID pinged for confirmation. The payment went through via a local food co-op token she’d earned last week moderating a neighbourhood assembly on urban gardens. Her vote and contribution had been recorded on a civic chain built by a small team in Milan.

Mira sat by the window and opened her laptop. A self-hosted Nextcloud instance came to life, syncing with her group’s latest files. No Big Tech in sight — just clean, open infrastructure. A Matrix chat notification popped up: her collaborators from Portugal and Croatia were online, reviewing edits on the climate resilience proposal they were drafting together. Everything was timestamped, verified, and logged through a lightweight governance tool running on IPFS.

A few streets away, her friend Lien was setting up for an art show. Mira had helped her mint digital certificates of authenticity for her physical paintings using a modest NFT registry on Arweave. Ownership, provenance, and purpose, tied together in a transparent thread.

Later, Mira walked past a street artist playing the guitar and singing near Place Sainte-Catherine. She smiled, tapped her phone gently to a sticker on his guitar case — a small payment flowed through using a Euro-pegged stablecoin built by a local digital commons project. No bank, no app — just address-to-address.

When she arrived home, Mira logged into a decentralised virtual world. Her decentralised identity authenticated her instantly — no password, no friction. Her avatar, which she owned and carried seamlessly across different virtual worlds, materialised in a bright, bustling plaza.

Waiting for her was a message from the street artist. He had uploaded a song just for her, a thank-you gift tucked inside the virtual world's open music corner. Mira smiled as the familiar guitar tones filled her headphones. It was a small, shimmering proof that relationships, creativity, and community could thrive in these new digital spaces too.

This story -while fictional- is not science fiction. Almost all technical elements are already there. But between technical possibility and reality stand regulation, markets and consumer adoption. Europe, and the European Commission are indispensable in making this story become reality.

4.1.1 Introduction: The Promise and Peril of Immersive Technologies

The emergence of Immersive Technologies¹ represents one of the most profound transformations in the history of the internet. Where Web 1.0 offered static content, and Web 2.0 enabled interactive platforms, Web 3.0 introduced cryptocurrencies and decentralised architectures, Web 4.0 envisions an immersive, intelligent, and persistent environment where digital and physical worlds merge seamlessly. The European Commission [defines Web 4.0](#) as “using advanced artificial and ambient intelligence, the internet of things, trusted blockchain transactions, virtual worlds and Extended Realities (XR) capabilities, where digital and real objects and environments are fully integrated and communicate with each other, enabling truly intuitive, immersive experiences.”

This integration brings with it immense potential for societal progress, but also immense risk. It is, therefore, essential to situate the conversation around Web 4.0 not simply in terms of technological innovation but also in terms of governance, ethics and trust.

4.1.1.1 The Promise of Immersive Technologies

The potential benefits of Immersive Technologies span multiple domains:

- **Education and Skills Development:** Immersive learning environments can offer real-time simulations, language practice, and cross-border collaborative classrooms. Students in rural or underserved regions can access high-quality educational resources through XR, reducing inequalities.
- **Healthcare and Well-being:** Virtual therapies for post-traumatic stress disorder, anxiety, and rehabilitation are already demonstrating efficacy. Immersive environments can promote mindfulness, support ageing populations through cognitive stimulation, and even assist in physical rehabilitation by tracking movement in real time.

¹ Immersive Technologies is the term used in this document is [defined by the OECD](#) as “technologies that aim to create digital experiences that are more interactive, engaging and realistic, with a greater degree of sensory immersion and spatial interaction, compared to other online experiences”

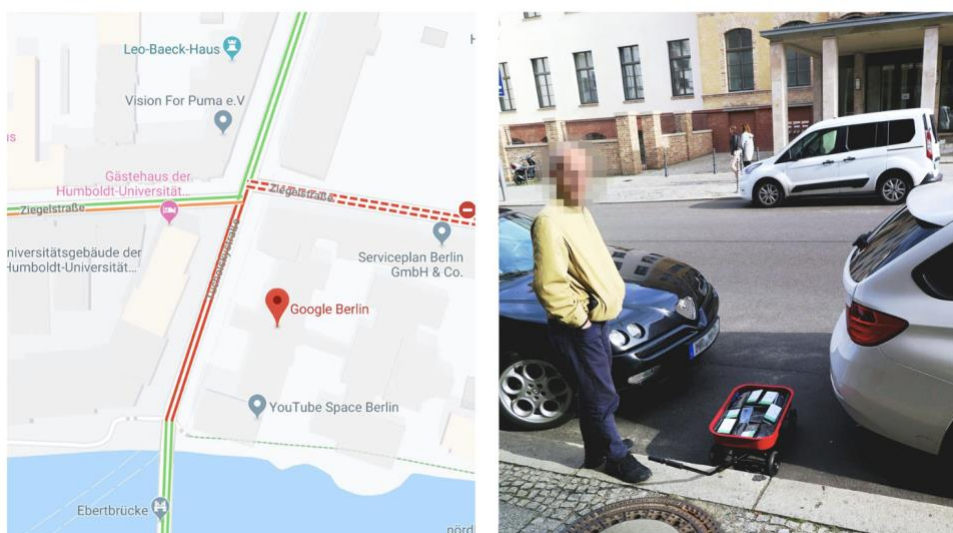
- **Economic Innovation:** Virtual marketplaces allow SMEs to reach global audiences. New forms of digital labour -such as design of virtual goods, immersive cultural production, and remote technical collaboration- create jobs and entrepreneurial opportunities.
- **Cultural and Social Life:** Mixed reality enables citizens to engage in cultural experiences beyond physical constraints. Virtual concerts, museums, and community gatherings can enhance inclusivity and cultural exchange.
- **Environmental Sustainability:** By reducing the need for travel and enabling virtual work environments, mixed reality can lower carbon emissions. Simulation technologies can model environmental interventions before real-world deployment.
- **Democratic Participation:** Virtual assemblies and deliberative platforms allow citizens to participate in policymaking processes across borders. Properly designed, these can broaden democratic inclusion and foster transnational civic engagement.

4.1.1.2 The Peril of Immersive Technologies

The risks of Immersive Technologies are equally profound:

- **Surveillance Capitalism on Steroids:** XR devices continuously collect sensitive biometric and behavioural data. Unlike web browsing, which produces discrete data points, immersive environments capture constant streams of information about movement, gaze, gestures, emotional responses, and potentially neural signals.
- **Algorithmic Manipulation:** Algorithmic recommendation engines, already problematic in social media, become even more powerful in immersive contexts. Already in a very innocent application like Google Maps, we can see the real-time manipulation of traffic through data collected and interpreted.

Hyper-personalisation risks creating algorithmically curated realities that fragment public discourse and undermine democratic deliberation.



Immersive Technology and Manipulation in Action: Google Maps Hack by Simon Weckert 2020²

- **Platform Concentration:** Without regulatory safeguards, immersive technologies could be dominated by a few corporate actors that control identity, assets and content. Closed,

² Simon Weckert is a German artist who created this performance and installation art piece in which he pulled a cart with 99 smartphones all running Google Maps through the streets of Berlin. While he was walking, the streets turned red and traffic was diverted allowing him to walk in the middle of the street. See: <https://www.simonweckert.com/googlemapshacks.html>

proprietary ecosystems would lock in users and prevent interoperability, leading to digital feudalism rather than digital democracy.

- **Digital Inequalities:** Access to high-quality XR devices and networks may be unevenly distributed, exacerbating social divides. Vulnerable populations may be excluded from opportunities while also being disproportionately targeted for exploitation.
- **Mental Health and Safety Risks:** Prolonged immersion risks physical strain, addiction, harassment and exposure to harmful content. Unlike 2D social media, where users can disengage, immersive harassment is experienced viscerally and can cause long-lasting trauma.
- **Legal Ambiguities:** Who is accountable for harms in decentralised environments? How do we regulate DAOs, NFTs or cross-platform identity systems? The absence of clarity undermines trust and creates risks of abuse.

4.1.1.3 Europe's Responsibility

The EU has both an opportunity and an obligation to ensure that Immersive Technologies evolve in line with European values. Its regulatory model has already shaped global digital norms, with the GDPR establishing data protection as a fundamental right. Europe's unique strength lies in its ability to align technology governance with social values, combining regulatory frameworks with participatory processes and multistakeholder engagement.

By investing in trust tools, the EU can:

- Protect citizens' fundamental rights in immersive environments
- Empower SMEs to compete in global digital markets on fair and ethical terms.
- Ensure democratic accountability in environments increasingly mediated by algorithms and immersive infrastructures.
- Position itself as a leader in the global debates on internet governance, ensuring that Web 4.0 remains open, interoperable and rights-based.

4.1.2 The Governance Challenge: Trust as Enabler

Trust is not only a normative principle but a practical enabler of governance. It represents the glue that binds digital transactions, immersive interactions, and decentralised communities into coherent, functioning systems. In Immersive Technology societies, where human experience is increasingly mediated by digital infrastructures, the question is not whether governance should be trust-based but how trust can be embedded in both regulation and technology.

4.1.2.1 Legal and Regulatory Foundations in the EU

The EU already has a strong regulatory landscape that can serve as a foundation for trust tools. However, each framework requires adaptation to meet the unique challenges of immersive, persistent and decentralised environments.

- **GDPR:** The General Data Protection Regulation provides the cornerstone for user control over personal data. Its provisions on consent, transparency, and purpose limitation are highly relevant to immersive technologies. Yet XR introduces new forms of sensitive data—biometric, neurological, emotional—that stretch the definitions and protections foreseen in 2016. Enforcement in decentralised architectures is also problematic: who is the data controller in a DAO? Can avatars be considered personal data? These questions demand clarification.

- **eIDAS 2.0:** The revision of the eIDAS Regulation creates a European Digital Identity framework, including digital wallets. This offers opportunities for verifiable credentials in virtual worlds. However, today's eIDAS is primarily centralised, relying on trusted state or corporate issuers. In contrast, Web 4.0 calls for hybrid models where decentralised identifiers (DIDs) can coexist with state-backed IDs. Without such integration, users will be forced to juggle incompatible identity systems across platforms.
- **Digital Services Act (DSA):** The DSA mandates transparency and accountability for large online platforms. Its provisions on algorithmic audits, systemic risk assessments, and content moderation create a precedent for immersive environments. Yet immersive harms are more subtle than text-based harms: harassment in VR feels more visceral; manipulative nudging in AR may be harder to detect. Regulators will need new competences and tools to monitor immersive environments.
- **Markets in Crypto-Assets (MiCA):** MiCA introduces legal certainty for crypto-assets, including stablecoins. In virtual worlds, NFTs and tokens can underpin ownership of virtual property, from avatars to land. MiCA provides guardrails but does not yet address how tokens interact with identity, consumer rights, and taxation across borders. Clarification is needed to prevent fraud and ensure sustainability of virtual economies.
- **AI Act:** The AI Act introduces a risk-based approach to algorithmic systems. High-risk AI must meet requirements of transparency, robustness, and human oversight. In immersive environments, AI systems for moderation, recommendation, or biometric analysis could qualify as high-risk. Linking AI Act obligations with immersive-specific safeguards is a priority.

4.1.2.2 International Comparisons

Europe is not alone in grappling with these challenges. Comparing EU efforts with other jurisdictions offers insights.

United States: The U.S. landscape is transitioning from regulatory fragmentation toward more structured oversight. The **GENIUS Act** serves as a cornerstone for stablecoin regulation, while executive and legislative initiatives signal broader alignment toward integrated digital-asset policy. Still, enforcement remains dispersed, and the future shape of federal policy—and its compatibility with EU frameworks like GDPR, eIDAS2, DSA, and MiCA—remains uncertain.

Japan: The "Metaverse Principles" embody democratic values, inclusivity, and human rights, while concurrently serving industrial-strategic objectives. The government relies on soft-law measures—including study groups within the Ministry of Internal Affairs and Communications and a public-private Cabinet Office council—to define, monitor, and regulate metaverse content. Amendments such as the extension of the Unfair Competition Prevention Act to virtual counterfeit goods illustrate Japan's adaptive legal approach. Critically, Japan's governance framework explicitly recognises creators as key stakeholders—reflecting a policy orientation that fosters innovation and cultural content production. Embedded within the broader Society 5.0 strategy, the metaverse is envisioned as part of a transformative infrastructure, leveraging immersive technology for societal resilience and wellbeing.

South Korea: Embracing a dual strategy of **vigorous industrial promotion** and **ethical governance**, South Korea has enacted the world's first standalone metaverse law—the *Virtual Convergence Industry Promotion Act*—which combines flexible regulation with self-regulatory oversight and impact assessment systems. Soft-law ethical principles undergird this framework. Substantial public investment, cultural innovation, and public-private partnerships are driving immersive platforms (e.g., Zepeto, ifland, Metaverse Seoul), amplified by strong consumer acceptance and new institutional linkages between creative industries and research. Regulatory momentum now extends to **virtual-asset oversight**, with impending rules on cross-border transactions from 2025.

China: China's metaverse approach is characterised by **state-led industrial strategy**, prioritising economic integration over consumer escapism. The **MIIT-led Three-Year Action Plan (2023–2025)** orchestrates development of core technologies (AI, blockchain, digital twins, identity systems), **industrial metaverse adoption** in manufacturing and service contexts, and the construction of immersive lifestyle applications. Governance is anchored by the **CAC**, operating within the broader regime of the **Cybersecurity Law, DSL, and PIPL**, ensuring metaverse platforms conform with political values and data sovereignty mandates. Unlike EU or U.S. models, China rejects crypto-driven metaverse economies, instead promoting a **domestic, utility-driven ecosystem** that is regulatory segmented and largely disconnected from global interoperability. While significant research and deployment capacity exist, ethical considerations such as algorithmic bias and equitable access remain emergent concerns.

These comparisons show that Europe's strength lies in aligning technological ambition with normative clarity. Unlike other regions, the EU can leverage its regulatory frameworks as a source of competitive advantage, turning trust into a market differentiator.

A more comprehensive international comparison can be found in Appendix 1

4.1.2.3 Risks of Fragmentation

The absence of a coherent trust framework risks fragmenting the internet into “splinternets”:

- **Technical Fragmentation:** Closed ecosystems prevent data, assets, and identities from flowing across platforms. A user's avatar in one world may be unusable in another, undermining interoperability.
- **Normative Fragmentation:** Competing governance models may split the internet into authoritarian-controlled versus democratic-controlled spheres. This would weaken global interoperability and values-based governance.
- **Institutional Fragmentation:** Within the EU, misalignment between regulations (e.g. GDPR vs. MiCA vs. eIDAS) risks creating overlapping or contradictory obligations. Internationally, lack of coordination with multistakeholder fora (ITU, OECD, WSIS) could undermine Europe's influence.

4.1.2.4 The Multistakeholder Imperative

Regulation alone cannot manufacture trust—it must be co-created across government, industry, civil society, academia, and citizens. The EU's **Markets in Crypto-Assets Regulation (MiCA)** provides essential guardrails for digital finance, but it does not by itself resolve questions of identity, consumer rights, or cross-border taxation. Similarly, trust in emerging “virtual worlds”—from immersive environments to decentralised digital ecosystems—depends not only on enforceable rules but also on social legitimacy and technical coherence. The EU's leadership in the **World Summit on the Information Society (WSIS+20) review**, which in 2025 assesses twenty years of global progress on inclusive information societies, highlights the need for **multistakeholder governance**. This process brings together UN agencies, governments, private sector actors, academia, and grassroots groups to define principles for a trustworthy digital future. Embedding trust into virtual worlds will require **collaboration across multiple layers**:

- **Standards bodies** such as the [World Wide Web Consortium \(W3C\)](#), which maintains web interoperability; [IEEE](#), which develops technical and ethical frameworks for emerging technologies; and the **International Organization for Standardization (ISO)**, which provides quality and safety benchmarks.

- **Regulatory agencies** at EU and national levels, including data protection authorities and financial supervisors, to enforce rights-based guardrails.
- **Grassroots communities**, including open-source developers, decentralised autonomous organisations (DAOs), and digital rights networks, to embed legitimacy and user empowerment into practice.

Together, these actors form a distributed architecture of trust. Without such collaboration, virtual worlds risk becoming fragmented landscapes -some highly regulated and centralised, others ungoverned and opaque- undermining confidence and adoption across borders.

4.1.2.5 The Role of Trust Tools

Trust must be operationalised. High-level commitments are necessary, but without practical instruments they risk remaining aspirational. Operationalisation means creating tools that embed trust directly into the digital infrastructure:

- **Interoperable identity and credential systems:** The proposed **European Digital Identity (eIDAS 2.0)** framework introduces EU-wide *digital wallets* that can store identity credentials, qualifications, and payment methods. If made interoperable across borders and sectors, such systems can anchor trust in both financial transactions and virtual environments.
- **Transparency and audit mechanisms for AI:** The **EU Artificial Intelligence Act** requires explainability, risk classification, and oversight for high-risk AI systems. Developing *technical auditability* and *continuous monitoring* mechanisms will be crucial for sustaining public confidence as AI systems become embedded in daily life.
- **Certification and labelling schemes:** Initiatives like the **Cybersecurity Act** create EU-wide certification frameworks for ICT products and services. Extending this logic to *virtual worlds*, *AI applications*, and *tokenised assets* can provide consumers with visible assurances of security, privacy, and fairness.
- **Regulatory sandboxes for experimentation:** The **EU Digital Finance Package** promotes regulatory sandboxes that allow innovators to test products under supervision. Extending sandbox models to AI, immersive environments, and decentralised finance would support innovation while embedding regulatory feedback loops early.

These instruments transform abstract values -transparency, accountability, fairness- into **enforceable and scalable practices**. The EU must ensure that their design and implementation reflect **European values of human dignity, democracy, and social inclusion**, rather than defaulting to either *market-driven standards* (as in the US) or *state-centric control* (as in China). In doing so, the EU can position itself as a **global standard-setter** for trustworthy digital ecosystems.

4.1.3 Evidence and Case Insights

The operationalisation of trust tools must be grounded not only in theory but also in empirical evidence. The OPENVERSE consultations, the EUBOF report, and related EU and OECD studies provide a rich foundation. Together, they reveal how stakeholders perceive risks and opportunities, what tools are most urgently needed, and how policy instruments can be designed to meet diverse societal needs.

4.1.3.1 Stakeholder Questionnaire Findings

The stakeholder consultations (Deliverables D3.1–D3.5) gathered perspectives from academic experts, SMEs, industry representatives, and policymakers. These insights can be organised across the thematic axes of governance, verification, inclusivity, business models, risk mitigation, and scalability.

- **Governance (Q1–Q3):** INS highlighted that governance principles such as human-centricity, inclusion, and privacy-by-design must be the baseline for trust. IDC added that multi-stakeholder governance, anti-discriminatory design, and behavioural norms were equally important. These findings confirm that trust cannot be left to private actors alone but must be rooted in EU-level governance principles. Stakeholders consistently raised the absence of interoperable identity and consent systems as a major gap undermining trust today.
- **Verification Tools (Q2):** There was broad consensus that interoperable identity frameworks and reputation systems are urgently needed. INS emphasised that such frameworks should be usable across platforms and jurisdictions. VUB's work on XR in collaborative robotics showed that while trust was not diminished by immersive interfaces, adoption would require verification tools to prevent abuse and ensure safety. This suggests a clear policy window for developing EU-backed verification schemes.
- **Legal Instruments (Q3):** Stakeholders pointed to GDPR, eIDAS, and the DSA as latent trust enablers. Yet they also underlined gaps: GDPR does not cover immersive biometric data in sufficient depth, eIDAS has not yet been integrated with decentralised identity models, and the DSA does not address real-time immersive interactions. These gaps must be filled to avoid trust erosion.
- **Co-Design and User Experience (Q4–Q5):** INS and VUB used participatory methods to include SMEs, policymakers and workers in XR scenarios. The feedback highlighted ergonomic concerns, the need for intuitive interfaces, and the importance of inclusivity benchmarks. VUB's survey found that immersive AR increased perceived enjoyment and social influence, without decreasing trust. This supports the argument that co-design and user-centred design are key enablers of trust.
- **Business Models and Risks (Q6–Q7):** INS noted that ethical business models place privacy and user sovereignty at their core. This requires new economic paradigms: data cooperatives, privacy-as-a-service, and business models where users control their digital assets. Stakeholders identified trust-eroding risks including opaque AI, misuse of biometric data, and platform manipulation. Ethical audit trails, explainability protocols, and consumer protection schemes were proposed as safeguards.
- **Scalability and Policy Integration (Q8–Q10):** INS stressed that their concepts were explicitly designed for scalability across jurisdictions. IDC warned of technical and economic barriers to adoption. VUB underscored hardware and comfort issues, while recognising the potential for AR to increase social influence and enjoyment. All agreed that EU-level trust frameworks and regulatory sandboxes would help overcome fragmentation.

4.1.3.2 EUBOF PESTLE Analysis

The EU Blockchain Observatory and Forum offered a structured PESTLE analysis of open virtual worlds:

- **Political:** Decentralised worlds lack centralised authorities to lobby for regulation. This risks leaving the field to corporate-controlled, closed platforms. International cooperation is essential to develop uniform standards for digital assets, governance, and identity. EU leadership is vital to prevent democratic values being marginalised by authoritarian or corporate governance models.

- **Economic:** Adoption depends on robust macroeconomic conditions. Current instability and rising interest rates slow investment in immersive infrastructure. Income disparities could further exclude vulnerable groups from participating. Taxation and regulatory frameworks for digital assets will determine whether virtual economies are transparent and stable or vulnerable to fraud and speculation.
- **Social:** Societal comfort with immersive interactions has grown since the COVID-19 pandemic normalised remote collaboration. Yet digital literacy gaps, privacy concerns, and norms around screen time remain barriers. Exclusionary effects could emerge if immersive technologies are affordable only to privileged populations. Cyberbullying and harassment risks are heightened in immersive contexts.
- **Technological:** Open virtual worlds require advanced networks (5G/6G), decentralised storage, powerful VR/AR devices, and blockchain scalability. Persistent challenges include interoperability between platforms, energy efficiency of blockchains, and ergonomics of XR hardware. EUBOF notes that without interoperability, user experiences will remain fragmented.
- **Legal:** GDPR offers a baseline, but immersive data raises new questions about sensitive categories. Intellectual property disputes over virtual assets, identity theft in immersive environments, and cross-border cybercrime are pressing challenges. DAOs further complicate accountability by diffusing decision-making power.
- **Environmental:** Immersive environments rely on energy-intensive infrastructure. Hardware production, data centres, and blockchain transactions all contribute to carbon footprints. Circular economy models, energy-efficient consensus mechanisms, and renewable energy integration are necessary to align open virtual worlds with Europe's sustainability goals.

4.1.3.3 Case Studies

Several illustrative cases highlight the opportunities and challenges of trust tools:

- **VUB XR Warehouse Study:** This experiment in warehouse logistics found that AR interfaces enhanced enjoyment and social influence among workers. Importantly, trust was not diminished, showing that immersive technologies can be introduced without eroding worker confidence if thoughtfully designed. However, ergonomic and comfort issues limited adoption, emphasising the need for inclusive design.
- **Ready Player Me:** This cross-platform avatar project shows the promise and limits of interoperability. While it enables avatars to move across multiple virtual worlds, rendering standards remain inconsistent, and asset transferability is partial. This underlines the need for EU-led standards on interoperability.
- **DAOs in Virtual Real Estate:** Early DAOs managing virtual land illustrate democratic governance possibilities. Members can vote on development and usage decisions, showing the potential of algorithmic democracy. Yet accountability remains unclear: if a DAO decision leads to harm, who is responsible? This legal ambiguity illustrates why regulatory sandboxes are essential.
- **International Strategies:** Japan's metaverse principles emphasise democratic values, South Korea's strategy prioritises industrial growth, and China integrates immersive tech into state control mechanisms. Europe must position itself clearly as the champion of openness, inclusivity, and trust.

4.1.3.4 Expert Interviews

We conducted four expert interviews with representatives from Siemens, Namirial, PixelPai and Indigo Ventures. Their answers -in synthesis and without attribution- are synthesised below and grouped in

specific issues. This synthesis reflects both the **technical-practical insights** (interoperability, certification, hybrid models) and the **broader governance principles** (human-centricity, privacy, inclusivity) that emerged consistently across the interviews. For the full list of interview questions, please refer to Appendix II.

1. Most pressing trust challenges

The lack of a federated and interoperable trust infrastructure is seen as the key challenge. This gap manifests in unreliable user identification, difficulties in verifying content provenance, and weak data governance frameworks across borders. Governance decentralisation is lagging, leaving accountability gaps and opacity around sources. Certification and verification are repeatedly cited as necessary but underdeveloped.

2. How users and communities establish trust, and limitations

In business contexts, trust is primarily contractual and institutionally anchored (B2B supply chains, regulated services). By contrast, consumers rarely demand transparency, and in many regions users rely on informal social cues or platform policies. The limitation is that most virtual platforms remain disconnected from formal trust infrastructures (eIDAS, qualified signatures). Regional differences persist, and there is little consumer pull for deeper transparency.

3. Company-developed trust tools

Examples include interoperable digital identity wallets, qualified seals and timestamps for digital content, and remote authentication solutions designed for high-integrity contexts. Previous experience from traceability in food supply chains and industrial settings is being repurposed, but such tools are not yet widely embedded in consumer-facing virtual worlds.

4. Role of decentralised technologies

Blockchain, verifiable credentials (VCs) and zero-knowledge proofs (ZKPs) are considered strategic complements rather than replacements. Hybrid models are preferred, where multiple certification authorities co-exist. VCs, as seen in COVID apps, illustrate potential scalability. Blockchain adoption in industrial metaverse contexts remains limited, but integration with regulated trust services is under exploration.

5. Trade-offs between openness, privacy, interoperability and safety

Interviewees acknowledge a tension: openness and decentralisation often dilute accountability, while strong accountability tends to reinforce centralisation. Contracts dominate industrial applications, whereas smart contracts are viewed with caution. Interoperability is pursued through federated and governed systems (e.g. NVIDIA Omniverse), balancing technical openness with defined governance boundaries.

6. Barriers (technical, regulatory, cultural)

Technologies hyped in 2018 (blockchain, VR) did not scale as expected. Governance decentralisation lags behind technical innovation. Regulatory fragmentation (inside and outside the EU) slows adoption, particularly in the absence of Mutual Recognition Agreements. Market pull from consumers is weak, organisational inertia persists, and infrastructure costs remain high. Decentralised communities often resist state-recognised mechanisms.

7. Evaluating trust tools

Metrics mentioned include volume of qualified transactions, onboarding and conversion times, compliance audits, and feedback from institutional users. Broader societal trust metrics are underdeveloped and not systematically applied.

8. Governance model preference

A hybrid governance model is widely favoured: public frameworks (GDPR, eIDAS, CRA) for certainty and rights enforcement; private sector and standards bodies for innovation and agility; multistakeholder oversight for high-risk or cross-border areas. Multi-certification-authority systems (e.g. TÜV, BaFin, universities) are viewed as resilient and exportable beyond Europe.

9. Future-essential trust tools and infrastructures

Interviewees converge on the need for:

- Government-backed decentralised infrastructures (e.g. EBSI/Eurostack).
- Interoperable digital identity wallets.
- Legally valid digital content certifications.
- Probabilistic trust signals.
- Privacy-preserving cryptography (ZKPs, anonymous credentials).
- Post-quantum secure trust layers, given the risk of “harvest now, decrypt later” attacks.

10. Recommendations to policymakers and standards bodies

Key recommendations include:

- Build and fund cross-border public trust infrastructures.
- Ensure GDPR-style user rights and privacy-by-design remain core.
- Promote governed decentralisation with multiple certifying actors.
- Extend eIDAS through *global* Mutual Recognition Agreements.
- Support sandboxes and pilots (identity, wallet integration, IPR governance, AI transparency).
- Learn from rapid Verifiable Credential rollouts during COVID as a model for scaling interoperable trust.

4.1.3.5 Synthesis

Taken together, the interviews confirm and extend the evidence presented in Sections 3.1–3.3. Four lessons stand out:

1. **Trust can be designed** through robust identity systems, audit trails, and participatory governance.
2. **Trust requires inclusivity**: ensuring immersive technologies are accessible, affordable, and safe across social groups.
3. **Trust must be safeguarded** via legal clarity, ethical certification, and effective enforcement.
4. **Trust only scales with interoperability**: without common standards, fragmentation will erode confidence and limit uptake.

The challenge for European policymakers is to translate these lessons into actionable design principles and regulatory instruments. This is addressed in the following section.

4.1.4 Design Principles and Practical Trust Tools

Embedding trust in Immersive Technologies requires more than broad commitments. It demands the design and deployment of specific tools—technical, legal, organisational—that operationalise principles such as privacy, accountability, inclusivity and transparency. In this section, we present a detailed exploration of the most critical trust tools, their design principles, and their implementation pathways.

4.1.4.1 Interoperable Identity and Credentials

Identity is the cornerstone of trust. Without reliable identity systems, users cannot authenticate themselves, verify others, or establish accountability. Yet today's identity frameworks are fragmented: some are centralised (e.g., platform logins), others are federated (OAuth systems), and a growing number are decentralised (blockchain-based DIDs). None offer seamless cross-platform interoperability.

- **Decentralised Identifiers (DIDs):** Allow individuals to create and control their own digital identities without relying on a single provider. DIDs can be anchored on blockchains, ensuring immutability and verifiability.
- **Verifiable Credentials (VCs):** Digital attestations of attributes (e.g., age, qualifications, memberships) that can be shared selectively, enabling privacy-preserving identity verification.
- **Hybrid Integration with eIDAS 2.0:** To ensure adoption, decentralised IDs must integrate with state-backed digital identities. A European digital wallet linked to DIDs and VCs would combine institutional trust with user autonomy.
- **Portability Across Platforms:** Standards such as W3C's Verifiable Credentials and initiatives like the Trust over IP stack should be adopted to enable movement of identities across virtual worlds.

Design principle: identity systems must empower the user with control, enable interoperability across platforms, and provide cryptographic assurance of authenticity.

4.1.4.2 Trust Labels and Certification

Users need clear signals about which platforms and services are trustworthy. A European Trust Label could serve this purpose.

- **Scope of Certification:** Criteria could include privacy protections, accessibility compliance, algorithmic transparency, sustainability measures, and inclusivity benchmarks.
- **Implementation:** Independent auditing bodies, supervised by EU institutions, would certify compliance. The process could mirror CE labelling for consumer products.
- **Benefits:** Trust labels would provide market incentives for compliance, empower users with choice, and create reputational value for ethical platforms.
- **Challenges:** Avoiding superficial “ethics washing” requires rigorous, transparent auditing processes.

Design principle: certification must be transparent, verifiable, and embedded into consumer choice architectures.

4.1.4.3 Ethical Audit Trails and AI Explainability

In immersive environments, AI systems curate experiences, moderate behaviours, and shape interactions. Without transparency, these systems can manipulate users, spread misinformation, or perpetuate bias.

- **Audit Trails:** Blockchain-based ledgers can record algorithmic decisions and moderation actions in tamper-proof formats. This allows regulators, auditors, and users to track how decisions were made.
- **Explainability Protocols:** AI systems must offer plain-language explanations for their outputs (e.g., why a certain avatar was flagged, why specific content was recommended). Technical documentation should also be available for regulators.
- **Integration with AI Act:** High-risk AI systems in immersive contexts should be subject to mandatory audits and explainability requirements.

Design principle: transparency must be built into AI systems, not bolted on as an afterthought.

4.1.4.4 User Agency Mechanisms

Trust is sustained when users feel empowered rather than exploited.

- **Privacy Dashboards:** Interfaces that display, in real time, what data is being collected, how it is used, and with whom it is shared.
- **Consent Managers:** Tools that allow users to dynamically grant, withdraw or modify consent. For example, a user might consent to gaze tracking for accessibility purposes but not for advertising.
- **Harm Prevention Tools:** Safety features such as panic buttons, emergency exits from immersive spaces, harassment filters, and live moderation support.
- **Digital Well-being Features:** Timers and notifications to prevent overexposure, fatigue, or addiction.

Design principle: user empowerment must be embedded into interface design, ensuring autonomy and safety.

4.1.4.5 Business Models for Trust

Trust cannot thrive in business models that monetise manipulation or exploit surveillance. Alternative models must be promoted:

- **Data Cooperatives:** Users pool data voluntarily and negotiate terms of use collectively, ensuring shared value.
- **Privacy-as-a-Service:** Platforms offer premium services based on strict privacy protections, making privacy a competitive differentiator.
- **Tokenised Incentives:** Users are rewarded for contributing to governance, content moderation, or sustainability efforts.
- **DAO-based Governance:** Decentralised Autonomous Organisations allow communities to collectively manage platforms and resources.

Design principle: economic models must align with ethical principles, ensuring that profitability and trust are not in conflict.

4.1.4.6 Regulatory Sandbox Experimentation

Sandboxes allow controlled experimentation with new trust tools.

- **28th Regime Principle:** A pan-European legal framework enabling companies to test innovations under EU-level rules rather than 27 different national regimes.
- **Use Cases:** Cross-border verifiable credentials, blockchain-based audit trails, DAO governance models, and XR safety standards.
- **Evaluation Mechanisms:** Independent expert panels assess sandbox outcomes, focusing on scalability, inclusivity, and risks.
- **Scaling Pathways:** Successful sandboxed solutions can be fast-tracked into EU regulation or certification schemes.

Design principle: innovation and regulation must be co-developed, not sequenced, ensuring agility without sacrificing rights.

4.1.4.7 Scenarios of Trust Tools in Practice

Consider practical scenarios:

- **Cross-Border Education:** A student in Portugal uses a DID to access a French immersive classroom. Their credentials are verified instantly across borders via eIDAS 2.0 integration.
- **Virtual Marketplace:** A consumer in Germany purchases a digital artwork in a virtual gallery. An EU Trust Label assures them of authenticity, privacy, and fair terms.
- **AI Moderation:** An avatar in a pan-European assembly is flagged by AI for disruptive behaviour. The system generates an audit trail, allowing human moderators to verify and appeal decisions.
- **Workplace Safety:** A logistics worker in Poland uses AR glasses. A consent manager ensures biometric data is used only for safety monitoring, not performance scoring.

These scenarios show how trust tools can make immersive experiences empowering rather than exploitative.

4.1.5 Scalability, Interoperability and Policy Integration

Trust tools will only have transformative impact if they scale across platforms, sectors and jurisdictions. Inconsistent application or fragmented adoption risks undermining their effectiveness and legitimacy. The European Union has a unique opportunity to develop a common trust framework that operates not only within its internal market but also sets a benchmark for global governance.

4.1.5.1 The Imperative of Scale

Trust mechanisms lose power if they are siloed. A verifiable credential system that works only within one platform does little to empower users across their daily journeys. Similarly, audit trails or consent managers that differ by platform or Member State risk creating confusion. Scale requires three dimensions:

- **Horizontal Scale Across Platforms:** Users should be able to use their trusted identity and credentials across virtual worlds, marketplaces, and workplaces.
- **Vertical Scale Across Sectors:** Trust tools must operate across education, healthcare, culture, logistics, and finance.

- **Geographical Scale Across Borders:** European citizens should be able to use trust tools across the Single Market and in interactions with global partners.

4.1.5.2 The EU Trust Framework

The EU should formalise an integrated Trust Framework for Web 4.0, analogous to the Digital Single Market strategy. This framework would harmonise legal, technical, and governance aspects.

- **Core Components:** interoperable identity and credential systems, audit trails, consent managers, trust labels, and sandbox mechanisms.
- **Modular Architecture:** The framework should be modular, allowing Member States to adapt to local contexts while ensuring interoperability.
- **Governance Structure:** Managed by a multistakeholder body including EU institutions, Member States, civil society, and industry.

4.1.5.3 Integration with EU Instruments

Existing EU regulations provide the building blocks, but must be connected:

- **GDPR:** Expanded to explicitly cover immersive biometric and behavioural data. Clarification is needed on data controllers in decentralised environments.
- **eIDAS 2.0:** Extended to integrate decentralised identifiers and verifiable credentials.
- **MiCA:** Coordinated with consumer protection and taxation frameworks to regulate NFTs and virtual assets.
- **DSA:** Updated to account for immersive harms, harassment, and algorithmic manipulation.
- **AI Act:** Enforced with mandatory audits and explainability in immersive environments.
- **Data Act & Data Governance Act:** Integrated to enable data sharing while protecting privacy.

By aligning these instruments, the EU can create coherence and avoid duplication.

4.1.5.4 Alignment with Global Governance

Trust tools must not stop at European borders. Europe must project its values globally.

- **WSIS+20 Process:** Use the 2025 review as a platform to embed principles of openness, human rights, and interoperability into the global governance agenda.
- **Global Digital Compact:** Advocate for explicit recognition of trust frameworks as enablers of rights-respecting digital spaces.
- **OECD:** Promote anticipatory governance and interoperability standards through OECD's Digital Economy Papers and Global Forum on Technology.
- **ITU, ISO, IEEE, W3C:** Engage actively in technical standards-setting, ensuring European trust principles shape interoperability standards.

4.1.5.5 Preventing Splinternets

Fragmentation remains a real risk:

- **Authoritarian Splinternets:** States that prioritise surveillance and censorship may create incompatible virtual ecosystems.
- **Corporate Splinternets:** Closed ecosystems run by dominant firms could prevent cross-platform portability.

- **Regional Splinternets:** Competing regional frameworks could hinder interoperability, as seen in past struggles over telecom standards.

The EU must mitigate these risks by anchoring trust in global multistakeholder processes and bilateral digital partnerships (e.g., EU-Japan, EU-US TTC).

4.1.5.6 Scenario Analysis: Scaling Trust Tools

- **Best-Case Scenario:** By 2030, EU citizens carry interoperable digital wallets integrating DIDs, VCs, and eIDAS credentials. Trust labels are recognised globally, and EU-led audit standards for AI are adopted by OECD and ITU. Europe leads the world in setting human-centric norms.
- **Worst-Case Scenario:** Fragmentation prevails. Citizens are forced to manage multiple incompatible IDs, credentials are not portable, and corporate monopolies dominate immersive spaces. Europe becomes a consumer rather than a shaper of global standards.
- **Likely Scenario:** A hybrid environment emerges, with EU trust frameworks adopted in Europe and influencing some global fora, but challenged by competing authoritarian and corporate models.

4.1.5.7 Policy Integration Roadmap

2025–2027: Establish pilot sandboxes, launch European Trust Label, and expand eIDAS to integrate DIDs.

2027–2030: Scale trust frameworks across sectors; integrate AI Act audits into immersive contexts; develop EU-wide certification schemes.

2030 onwards: Promote global adoption through WSIS+20 follow-ups, OECD recommendations, and bilateral partnerships.

4.1.6 Conclusions and Recommendations

The evidence presented throughout this policy brief demonstrates a central conclusion: trust is not a luxury in the era of Web 4.0 but an essential infrastructure. Without trust, immersive environments will be shaped by monopolies, surveillance and manipulation. With trust, they can become engines of innovation, inclusion and democratic renewal. The European Union is uniquely placed to lead the world in embedding trust into the design of mixed reality societies.

4.1.6.1 Overarching Recommendations

1. **Adopt an EU Trust by Design Framework:** Anchor all immersive technologies in principles of human rights, inclusivity, privacy, and accountability. This framework should integrate GDPR, eIDAS, DSA, MiCA, AI Act, and Data Act into a coherent architecture.
2. **Launch EU Trust Tools Sandboxes:** Under the 28th regime principle, create cross-border environments where interoperable identity systems, AI audit trails, and DAO governance models can be tested.
3. **Establish a European Trust Label:** Certify platforms, organisations and services that meet EU trust standards, ensuring transparency, accessibility and ethical design.
4. **Leverage Blockchain and Decentralised Governance:** Support the adoption of DIDs, verifiable credentials, DAOs and smart contracts as enablers of openness, accountability and community empowerment.

5. **Strengthen Global Governance Engagement:** Position the EU as a norm entrepreneur in WSIS+20, OECD, ITU, ISO and other fora, ensuring that trust principles shape global standards.
6. **Ensure Sustainability and Inclusion:** Promote energy-efficient XR infrastructures, accessibility standards, and measures to bridge digital divides.
7. **Empower Regulators and Citizens:** Equip authorities with technical capacity to enforce compliance, and empower citizens with privacy dashboards, consent managers and redress mechanisms.

4.1.6.2 Policy Roadmap

2025–2027: Establish Trust Tools Sandboxes, develop certification criteria for the Trust Label, expand eIDAS to integrate DIDs, and create funding lines for inclusive XR research.

2027–2030: Scale trust frameworks across sectors, integrate immersive contexts into the AI Act and DSA, and embed Trust Labels into procurement and consumer markets.

2030 onwards: Promote the EU Trust Framework as a global benchmark, influencing WSIS+20 follow-ups, OECD recommendations, and bilateral digital agreements.

4.1.6.3 The Strategic Imperative

The EU must act now. Delay risks ceding control of virtual worlds to actors whose values diverge from Europe's. By investing in trust tools, the EU can protect citizens, empower SMEs, strengthen democracy, and secure sovereignty. Trust will not emerge spontaneously; it must be designed, tested, and scaled. Europe has the regulatory expertise, institutional capacity and normative vision to make this happen.

4.1.6.3.1 Final Note

Trust is the connective tissue of the future internet. Just as the Single Market created prosperity through harmonised rules for goods and services, so too can a European Trust Framework create confidence in digital and virtual interactions. If Europe leads, it can ensure that Web 4.0 remains open, inclusive, and rights-based. If it fails, the future may be defined by fragmentation and control. The choice is urgent, and the time to act is now.

5 CONCLUSIONS

The OpenVerse process moves from the understanding that **policy impact depends on evidence and engagement** in equal measure. Rigorous research establishes credibility, but it is the iterative dialogue with practitioners, innovators and public authorities that translates insight into actionable, legitimate policy recommendations.

The integration of **policy prototyping** within a Horizon Europe coordination and support action proved particularly valuable: it enabled direct testing of ideas, early identification of regulatory bottlenecks and the co-creation of solutions that reflect real-world conditions.

6 ETHICS COMPLIANCE SIGN-OFF AND PUBLIC BRIEF DPIA

Deliverable D7.5 – Second Policy Brief

Project: OPENVERSE – Governance and Trust in Virtual Worlds

Work Package: WP7 – Project Management and Ethics Governance

Ethics Review Date: 29 October 2025

Reviewed by: OPENVERSE Ethics Advisor – UNEXT Ltd

6.1 ETHICS COMPLIANCE SIGN-OFF

Deliverable D7.5 consolidates two policy briefs ‘Regulatory Sandboxes for Virtual Worlds Innovation’ and ‘Trust Tools for Immersive Technologies’ both developed through participatory and evidence-based consultation processes. It fully aligns with the EU Charter of Fundamental Rights, the General Data Protection Regulation (GDPR – Regulation 2016/679), and the AI Act (Regulation 2024/1689), demonstrating commitment to transparency, fairness, accountability, and responsible governance of immersive technologies.

The deliverable reflects GDPR principles of lawfulness, purpose limitation, and data minimisation. Personal data were processed solely for expert interviews and policy-prototyping sessions. Participants provided explicit informed consent, interviews were pseudonymised, and recordings were securely stored under restricted access. No data were transferred outside the EU, and outputs are published only in aggregated form. AI-assisted analysis was limited to anonymised data under human oversight, consistent with the AI Act’s limited-risk classification and transparency obligations.

Ethical Compliance Rating: ● High – Fully compliant with EU ethical and legal requirements.

6.2 MITIGATION ACTIONS REQUIRED

Area	Identified Risk	Mitigation Measure	Responsible Partner
Data Protection	Residual risk of re-identification through quotes	Maintain pseudonymisation logs and Ethics Advisor pre-publication review	WP7 / UNEXT
Consent Archiving	Traceability of signed consent forms	Encrypt and store separately from datasets	POLIMI
AI Use in Analysis	Ambiguity in AI-assisted tools	Maintain AI-use declaration annex in deliverables	UNEXT / POLIMI
International Dissemination	Cross-border policy data use	Confirm GDPR-compliant clauses in cooperation agreements	WP7 Coordinator
Ongoing Oversight	Monitoring of stakeholder-related data	Quarterly Ethics Committee review and DPIA update	UNEXT / WP7

Residual risks are minimal and already addressed through project-wide Ethics Committee oversight and Data Management Plan II (D7.7).

6.3 OVERALL ETHICAL ACCEPTABILITY EVALUATION

D7.5 demonstrates a mature ethical framework, integrating participatory and transparent methodologies aligned with the Horizon Europe Ethics Guide. All data-processing operations are lawful, limited, and consent-based. The policy-brief development process embodies procedural justice and accountability, while complying with the GDPR and AI Act transparency principles.

Overall Evaluation: ● Ethically Compliant – Low Residual Risk; Full GDPR and AI Act Alignment.

6.4 PUBLIC BRIEF DATA PROTECTION IMPACT ASSESSMENT (DPIA)

This public summary outlines how the OPENVERSE project ensures that personal data used in the development of D7.5 – Second Policy Brief – are processed lawfully, transparently, and securely in

accordance with the General Data Protection Regulation (GDPR – EU 2016/679) and the AI Act (Regulation 2024/1689).

6.4.1 Purpose and Context

D7.5 gathers expert insights through structured interviews, workshops, and co-creation exercises to inform European policy frameworks on virtual worlds governance. Data collection is minimal, targeting professional roles and opinions without storing sensitive personal identifiers.

6.4.2 Lawful Basis for Processing

Data processing is based on:

- Article 6(1)(a) GDPR – explicit consent of participants;
- Article 6(1)(e) GDPR – processing necessary for tasks carried out in the public interest (research);
- Article 89 GDPR – safeguards for research including pseudonymisation and limited retention.

6.4.3 Data Categories and Retention

Data Category	Description	Purpose	Retention
Interview Data	Professional name, organisation (optional)	Expert consultation for policy input	Stored encrypted until project end +5 years
Workshop Materials	Aggregated notes, insights	Policy analysis and recommendations	Anonymised after analysis
Recordings (optional)	Audio/video of sessions (with consent)	Internal reference only	Deleted upon participant withdrawal or project end
Metadata	Engagement statistics	Policy participation reporting	Anonymous, long-term archive for transparency

6.4.4 Risk Assessment and Mitigation

- Informed Consent: Participants received full disclosure and retained the right to withdraw at any time.
- Data Minimisation: Only professional contact data collected; no special category data.
- Pseudonymisation: All identifiers replaced before dissemination.
- Secure Storage: Data hosted on EU servers under encryption and restricted access.
- Oversight: Periodic review by the Ethics Committee and Data Protection Officer.

6.4.5 Residual Risk and Evaluation

After mitigation, the residual privacy risk is rated as low. D7.5 satisfies GDPR and AI Act transparency requirements, ensuring trustworthy, human-centric policy outcomes consistent with Horizon Europe's ethics framework.

Final DPIA Rating: ● Low Risk – Fully GDPR and AI Act Compliant.

6.4.6 5. Ethics Advisor Sign-Off

Name	Organisation	Role	Date
Fabio Perossini	UNEXT Ltd	OPENVERSE Ethics Advisor	29/10/2025
Alessandro Paciaroni	Lisbon Council	Deliverable Lead	29/10/2025

REFERENCES

- Attrey, A., Leshner, M., & Lomax, C. (2020). The role of sandboxes in promoting flexibility and innovation in the digital age. OECD Going Digital Toolkit Note, No. 2, https://goingdigital.oecd.org/data/notes/No2_ToolkitNote_Sandboxes.pdf
- Baldini, D., & Francis, K. (2024). AI Regulatory Sandboxes between the AI Act and the GDPR: The role of Data Protection as a Corporate Social Responsibility. CEUR Workshop Proceedings, 3731. <https://cris.maastrichtuniversity.nl/ws/portalfiles/portal/213129909/paper07.pdf>
- Buzzell, C., Lalji, Z., Loyola, A., Rants, K., Scofield, E., & Zimmermann, S. (2023). Unlocking Commerce in the MetaVerse. 8 June. McKinsey's E-Commerce Global Initiative. Retrieved from <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/unlocking-commerce-in-the-MetaVerse#/>
- Cantú, C., Franco, C., & Fro, J. (2024). The Economic Implications of Services in the MetaVerse. BIS Papers No 144, February. Bank for International Settlements. Retrieved from <https://www.bis.org/publ/bppdf/bispap144.pdf>
- CIPPIC, the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic University of Ottawa, Faculty of Law (2024), Making Privacy More than a Virtual Reality: The Challenges of Extending Canadian Privacy Law to Extended Reality. Retrieved from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2023-2024/p_202324_02/
- Crogman, H.T., Cano, V.D., Pacheco, E., Sonawane, R.B., & Boroon, R. (2025). Virtual Reality, Augmented Reality, and Mixed Reality in Experiential Learning: Transforming Educational Paradigms. Education Sciences, 15(3), 303. DOI: 10.3390/educsci15030303
- Di Porto, F., Ennis, S., & Foà, D. (2024). Emerging Virtual Worlds: Implications for Policy and Regulation. 22 February. CERRE Tech Media and Telecom report. Retrieved from <https://cerre.eu/publications/emerging-virtual-worlds-implications-for-policy-and-regulation/>
- Financial Conduct Authority (FCA) (2017). Regulatory Sandbox Lessons Learned Report. 20 October. Retrieved from: <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>
- Fu, J. (2022). Future Development and Regulations of MetaVerse and NFT in China. Available at SSRN: <https://ssrn.com/abstract=4159747> or DOI: 10.2139/ssrn.4159747
- Greenhill, A., & Fletcher, G. (2013). Laboring Online: Are There “New” Labor Processes in Virtual Game Worlds? Journal of the Association for Information Systems, 14(11) DOI: 10.17705/1jais.00346
- Hennig-Thurau, T., Aliman, D.N., Herting, A.M., Cziehso, G.P., Linder, M., & Kübler, R.V. (2023). Social interactions in the MetaVerse: Framework, initial evidence, and research roadmap. Journal of the Academy of Marketing Science 51, 889–913. DOI: 10.1007/s11747-022-00908-0

Korinek, A. (2023). MetaVerse Economics part 1: Creating Value in the MetaVerse. 6 June. Brookings Institution. Retrieved from: <https://www.brookings.edu/articles/MetaVerse-economics-part-1-creating-value-in-the-MetaVerse/>

Levy-Basse, S., & Fang, C. (2022). Banking on the MetaVerse: The Imperatives of Web 3.0 for Financial Services. Prophet Blog. Retrieved from: <https://prophet.com/2022/11/banking-on-the-MetaVerse-the-imperatives-of-web-3-0-for-financial-services/>

Madary, M., & Metzinger, T.K. (2016). Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology. Frontiers in Robotics and AI 3:3. DOI: 10.3389/frobt.2016.00003

Mathews, M., Mérey, T., Adigozel, O., & Busch, N. (2023). The Expanding Health Care MetaVerse. 9 May. Boston Consulting Group. Retrieved from: <https://www.bcg.com/publications/2023/the-expanding-reality-of-the-health-care-MetaVerse>

National Institute of Standards and Technology (NIST) (2024). Cyber Security Framework 2.0. Retrieved from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

OECD (2025a). An Immersive Technologies Policy Primer. OECD Digital Economy Papers No. 373, March (revised version: May). Retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/03/an-immersive-technologies-policy-primer_aa2e7910/cf39863d-en.pdf

OECD (2025b). Agile Mechanisms for Responsible Technology Development. OECD Science, Technology and Industry Policy Papers No. 176, April. Retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/04/agile-mechanisms-for-responsible-technology-development_84f0fcea/2a35358e-en.pdf

Parliament of Australia (n.d.). Emerging Challenges: AI and the MetaVerse. Retrieved from: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digitalplatforms/Report/Chapter_9_-_Emerging_challenges

Raja, U.S., & Al-Baghli, R. (2025). Ethical concerns in contemporary virtual reality and frameworks for pursuing responsible use. Frontiers in Virtual Reality 6: 1451273. DOI: 10.3389/frvir.2025.1451273

Smith, C.H., Molka-Danielsen, J., Webb-Benjamin, J.-B., & Rasool, J. (2025). The challenges of consent in a decentralised MetaVerse: exploring ethically informed protections and standards to safeguard humans. Frontiers in Virtual Reality 6: 1401073. DOI: 10.3389/frvir.2025.1401073

Trentini, Y.A. (2020). The Flourishing Internal Economies of Virtual Reality Worlds. 18 October. Medium. Retrieved from: <https://medium.com/vr-review/dollars-made-inside-different-vr-worlds-become-real-life-wealth-2ca94c17bedb>

Robertson, A., & Faife, C. (2022). A hacker stole \$625 million from the blockchain behind NFT game Axie Infinity. 29 March. The Verge. Retrieved from: <https://www.theverge.com/2022/3/29/23001620/sky-mavis-axie-infinity-ronin-blockchain-validation-defi-hack-nft>

Westphal, C., Hong, J., Kang, S.-G., Chiariglione, L., & Jiang, T. (2023). Networking for the MetaVerse: The Standardization Landscape. ITU Journal on Future and Evolving Technologies, 4(4), December, 604-618. DOI: 10.1145/641480.641521

XR Safety Initiative (XRSI) (2020). The XRSI Privacy and Safety Framework. Retrieved from: <https://xrsi.org/publication/the-xrsi-privacy-framework>

Zetsche, D.A., Buckley, R.P., Arner, D.W., & Barberis, J.N. (2017). Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. *Fordham Journal of Corporate & Financial Law*, 23(1), 31–103.

7 APPENDIX A

2025 OPENVERSE POLICY DIALOGUE

To Trust or Not to Trust?

How to Build a Trust-By-Design Architecture for Europe

Monday, 27 October 2025

10h30 to 12h45 CET

Online

As experts argue “trust is the missing layer of the digital age.” Immersive technologies (Web 4.0) are reshaping society by blending digital, physical and virtual experiences. They promise advances in education, healthcare, industry and civic life, but also pose new risks, such as surveillance, disinformation, concentrated platforms) that could erode public trust. Europe’s strong regulatory foundations can provide a basis to build a trust-by-design framework and address this issue.

A key policy tool is the regulatory sandbox: a controlled, time-limited testing environment where innovators can trial new products under regulator oversight. For virtual worlds, sandboxes can address complexities like persistent data, interoperability across platforms, and AI-driven interactions. Meanwhile, “trust tools” – such as decentralised identities, verifiable credentials and digital assets – are the key to build a European trust architecture by ensuring immersive technology is reliable and transparent. Regulatory sandboxes aren’t “one more regulatory burden.” When designed as lean, time-boxed, outcome-driven environments, with clear success criteria, proportionate safeguards, and mutual-recognition pathways, they can accelerate, not stall, the deployment of trust tools in immersive virtual worlds.

But how can regulatory sandboxes accelerate rather than stifle the deployment of trust tools in immersive virtual worlds? Which concrete policy solutions should we co-create and refine to enhance Europe’s readiness for Web 4.0? What pathways can deliver Europe-wide, cross-jurisdictional sandboxes that enable real-world testing of interoperable identity, ethical audit trails, trust labels, and related tools?

OpenVerse research finds consensus that interoperable digital identity is critical to trust in virtual worlds, and that without intervention “closed, corporate ecosystems” could fracture the internet. Establishing European trust tools sandboxes under the 28th regime principle to test these tools cross-border without conflicting national rules can prevent this from happening.

PROGRAMME:

10h30 to 10h35 Welcome

10h35 to 11h05 **Plenary: To Trust or Not to Trust? How to Build a Trust-by-Design Architecture for Europe**

Introduction:

- **Francesco Mureddu**, vice president, the Lisbon Council

Keynote:

- **Emanuela Girardi**, president, AI Data Robotics Association

Special Presentations:

- **Francesco Molinari**, senior research associate, the Lisbon Council
- **Arno Laeven**, executive director, European Decentralisation Institute

Moderator:

- **Arta Ertekin**, communication and dissemination specialist, Martel Innovate

11h15 to 12h45 **Policy Prototyping Session: Sandboxing Trust-by-Design in Europe**

The workshop will focus on policy prototyping, an innovative approach to co-developing practical solutions with key stakeholders. This session will gather policymakers, industry experts, and representatives from SMEs, start-ups, academia, member states and European institutions to design, prototype and stress-test actionable solutions to the regulatory challenges in the virtual worlds sector. The workshop will be based on preliminary recommendations of the policy briefs “Regulatory Sandboxes for Virtual Worlds Innovation: *A Framework for EU Leadership*” and “*Trust Tools for Immersive Technologies*.”

8 APPENDIX B

OpenVerse Dialogue

Policy Prototyping Design Playbook

What are we doing?

Move policy recommendations from **what** (policy research, recommendations in briefs) **to how** (stakeholders' lived perspectives and co-designed solutions). The aim is to:

1. Stress-test recommendations through stakeholder experience
2. Grasp user-level impacts (e.g. citizens verifying online, SMEs scaling services)
3. Generate feasible, scalable prototypes aligned with EU frameworks according to point 1 and 2 (DSA, AI Act, eIDAS 2.0, Virtual Worlds Strategy)

How are we doing it?

To achieve the objectives the session should be:

- **Stakeholder-centred:** focus on user journeys (citizens, SMEs, regulators)
- **Scenario-based:** use real-life cases to make abstract rules tangible
- **Iterative:** test, refine, feedback within the session

In concrete

1. Tap into empathy and storytelling, scenarios must become alive, not synthetic. Do not overdo it that will make it feel fake. Just add some emotional characterisation.
2. Linked to 1. - add mindsets and characters (e.g. a teacher wanting to teach but being overwhelmed by following technical and privacy operational guidelines and bureaucracy, children and their parents wanting the best for their kids and being wary of invasive tech, entrepreneurs wanting to test and bring their ideas to life and scale while coping with uncertainty etc.)
3. Link this to simple tasks (can be guiding questions)
4. Trace this back to the systemic change

The two scenarios

Scenario A – The Crossborder Worker

Objective:

Establish an approach for this scenario whereby a system reduces data requirements yet remains operational by leveraging decentralised technologies.

The story:

Ana, a technician from Portugal, arrives at an industrial site in Germany. She is eager to begin her assignment, but entry depends on showing she completed a mandatory Health and Safety course. At the gate, she presents her EU Digital Wallet on her phone. The supervisor scans the QR code of her verifiable credential. The screen flashes green: Ana is cleared for entry. The site's Head of Safety feels torn: his job is to enforce rules and protect workers, but every delay at the gate slows down the company's operations. The company owners want to grow cross-border, but fear that opening their sites to external workers without airtight verification could expose them to accidents, liability, or even IP loss if the wrong person gains access.

The tasks:

1. How can trust tools (eIDAS2.0 wallets, verifiable credentials, EU trust labels) ensure that both Ana and the supervisor feel secure and confident at the gate?
2. What safeguards would reassure company owners about safety, liability, and IP protection?
3. How can SMEs offering training avoid duplicating effort across member states and scale their services EU-wide?

Systemic change:

Sandbox pilots with interoperable diplomas and consent managers could lead to:

- Crossborder recognition of professional certifications (EBSI and eIDAS2.0)
- Real-time verification of credentials without having to contact the issuer of the credentials
- Regulatory pathways to embed recognition into EU law, strengthening labour mobility, protecting IP and cutting compliance costs for businesses while upholding safety

Scenario B – The 28th regime as a Virtual World

Objective:

Assess how XR, Blockchain, AI and other technologies can support the creation of a trustworthy virtual space where innovative startups, micro SMEs and mobile professionals residing in any EU Member State can do business and interact with public administration at various levels (including for regulatory compliance, access to procurement opportunities, job search, remote co-work and co-production etc.).

The story:

Teresa is an engineer and a middle school teacher. She is active in EU and international developer communities with expertise in cybersecurity. She decides to start a company with her husband and two colleagues from different European countries. The question arises: where should the new entity be registered? After considering traditional options, she recalls the 28th regime, now established as a virtual world - though she wonders about its feasibility, security, and trustworthiness.

The tasks:

What technologies and applications help Teresa and partners to:

1. Safely and repeatedly interact with public authorities to register and maintain their company in a European-wide registry
2. Enroll as employers, file annual tax declarations, and perform administrative tasks without needing a specific location in an EU country
3. Negotiate contracts, hire staff, sign deals, and conduct virtual payments with confidentiality and full protection
4. Securely pay bills, taxes, social security contributions, and other levies to the virtual "State"
5. Access tenders and reuse corporate profile information stored on the cloud, ensuring identification, privacy, and data protection
6. Exchange data and do transactions with other business/entities
7. Other key operational needs

Systemic change:

As a sandbox, the 28th regime would harmonise and neutralise conflicting national business laws to create an innovation-friendly environment that fosters growth, prosperity and scalability for EU startups and micro SMEs while preserving legal certainty and public accountability.

9 APPENDIX C

2025 OPENVERSE POLICY DIALOGUE

To Trust or Not to Trust?

How to Build a Trust-By-Design Architecture for Europe

Monday, 27 October 2025

SESSION REPORT

The OpenVerse Policy Dialogue brought together experts, researchers and policymakers to discuss one of the most urgent questions facing Europe's digital transition: how to embed trust-by-design principles into the foundations of emerging virtual worlds. The dialogue built on two forthcoming OpenVerse policy briefs - one focused on trust and another on regulatory sandboxes - and sought to translate these conceptual frameworks into actionable, evidence-based policy recommendations.

The session opened with a keynote presentation outlining how Europe can harness existing regulatory and ethical frameworks to ensure that immersive technologies evolve in ways that strengthen, rather than erode, public confidence. Subsequent presentations introduced two complementary briefs: one on trust tools for immersive environments, and another on regulatory sandboxes as policy instruments for experimentation within virtual worlds.

- **Trust as a Design Requirement**

Participants agreed that Europe's distinctive approach to technology governance - grounded in the rule of law and fundamental rights - provides a unique advantage in shaping trustworthy virtual worlds. Building trust requires transparency, human oversight, robustness, and secure data governance to be embedded at the design stage. Examples included audit trails, verifiable digital identities and AI-driven labelling of avatars or agents.

- **The European Path to Digital Leadership**

Speakers underlined that the European model of "trust by design" can be a global benchmark. It combines three interdependent pillars:

- **Standards**, ensuring interoperability across platforms
- **Skills**, empowering developers, policymakers and end-users to act responsibly
- **Security**, embedding privacy-enhancing technologies and resilient authentication in every layer of the digital stack

Trust, participants agreed, is not a brake on innovation but a competitive advantage - a defining feature of Europe's digital brand.

• Regulatory Sandboxes as Enablers of Safe Experimentation

The discussion on sandboxes emphasised their potential to reconcile innovation with accountability. By providing temporary, controlled environments where regulations can be tested and refined, sandboxes allow innovators and regulators to co-learn and co-design new governance models. The idea of a *European Sandbox for Virtual Worlds*, structured under the principles of the proposed 28th regime, was explored as a means to overcome legal fragmentation and accelerate cross-border innovation.

• The Global Dimension

Several interventions stressed the urgency of acting quickly. While the United States and Asia are advancing rapidly in immersive technologies, Europe has the opportunity to lead in governance. Participants called for investment in digital infrastructure, interoperability and ethical frameworks, rather than a narrow focus on industrial protectionism.

Policy Prototyping Breakouts

After the plenary, participants joined two parallel sessions to translate ideas into concrete policy prototypes.

Breakout 1: Trust in Practice

This group examined a scenario in which a worker presents digital credentials to access a cross-border industrial site. Discussions revealed several key takeaways:

- **Standardisation is crucial:** Both technological and procedural standards are needed so that a credential recognised in one member state is valid across all others
- **Certification of trust-tool providers** is essential to guarantee reliability and security
- **Training and awareness:** Users and verifiers alike must understand how trust tools work to ensure their proper use
- **Human oversight** remains indispensable. Trust mechanisms must be visible, meaningful and backed by clear political communication on the kind of digital society Europe aims to build

The group concluded that trust cannot be legislated into existence; it must be *operationalised* through shared standards, certification schemes and education.

Breakout 2: Sandboxes and the 28th Regime

This session explored how a “28th regime” - an optional, European-wide legal framework - could operate as a virtual environment for start-ups and innovators. Three layers were identified as building blocks for such an ecosystem:

- **Infrastructure**, ensuring technical interoperability through digital identities and data-exchange systems

- **Service layer**, defining harmonised administrative and regulatory processes for taxation, contracting and public procurement
- **User-centric layer**, safeguarding privacy, data ownership and transparency for citizens and entrepreneurs

Participants proposed that sandboxes could serve as phased testing environments for each of these layers, enabling gradual deployment and iterative learning. Cybersecurity and data-governance mechanisms would need to be embedded throughout.

Across both sessions, a coherent vision emerged: trust and innovation are mutually reinforcing. Building trustworthy virtual worlds requires interoperable standards, shared governance and active citizen engagement. Regulatory sandboxes can serve as the bridge between experimentation and regulation - the place where trust principles are tested, refined and scaled.

The discussions converged on a single insight: Europe's leadership in virtual worlds will depend not on the speed of technological adoption, but on the depth of trust it can inspire. By combining *trust by design* with *governance by experimentation*, Europe can build virtual environments that are open, secure and human-centric - and, in doing so, turn its values into a global competitive edge.

10 D. GLOSSARY OF USED TERMS

<i>Term</i>	<i>Meaning</i>
Artificial Intelligence (AI)	The simulation of human intelligence processes by machines, especially computer systems, enabling them to perform tasks such as learning, reasoning, and problem-solving.
Augmented Reality (AR)	A technology that overlays digital content—such as images, sounds, or information—onto the real-world environment in real time.
Block Chain (BC)	A decentralized, tamper-resistant digital ledger that records transactions across multiple computers in a secure and transparent manner.
Cybersecurity	The practice of protecting systems, networks, and data from digital attacks, unauthorized access, and other cyber threats.
Digital Sovereignty	The concept that individuals, organizations, or nations have control over their own digital data, infrastructure, and technologies without external dependence or interference.
Digital Twins	Virtual replicas of physical objects, systems, or processes that are used to simulate, monitor, and optimize their real-world counterparts in real time.
EU Policy	The framework of laws, regulations, and strategies established by the European Union on economic, social, environmental, and technological matters.
GDPR (General Data Protection Regulation)	A comprehensive EU regulation that governs the collection, processing, and protection of personal data, ensuring individuals' privacy rights.
Interoperability	The ability of different systems, devices, or applications to work together, exchange data, and use the exchanged information effectively and seamlessly.
MetaVerse (MV)	An evolving network of immersive, interconnected virtual environments where users can interact with each other and digital assets through avatars in real time.
OpenVerse	Open and co-created Virtual Worlds for Europe. A Coordination and Support Action funded by Horizon Europe. In this Policy Brief: An interconnected, user-centric MV/VW environment rooted in European values.
Safe Harbours	Legal provisions within a statute or regulation that provide protection from liability or penalties when certain specific conditions are met.
Technological Free Zones	Geographically located physical environments, in real or near-real settings, used for testing and experimenting with technology-based innovative processes, with direct and continuous monitoring by national regulatory authorities and other competent entities.
Virtual Reality (VR)	A computer-generated simulation that immerses users in a three-dimensional environment, often using headsets and motion tracking.
Virtual Worlds (VW)	Persistent, computer-simulated environments where users can interact with each other and digital objects through avatars.

11 E. COMPARATIVE TABLE: SANDBOX MODELS IN EU VS. GLOBAL JURISDICTIONS

Country	Sector Focus	Oversight Mechanism	Data Rights Framework	Key Distinctive Features
European models				
Germany	Industrial/Urban VWs	Federal Ministry for Economic Affairs (BMWK)	GDPR (waivers for testing)	Permanent legislative framework (<i>Reallabore-Gesetz</i>); cross-sectoral real-world testing
EU (BCSI)	Blockchain/Supply Chain	Multi-regulator EU/national dialogue	GDPR/eIDAS harmonized	Transnational sandbox; tests interoperability & digital identity across 27 member states
UK	Healthcare/Fintech	MHRA (health), FCA (finance)	UK GDPR	Sector-specific sandboxes; "Supercharged Sandbox" with NVIDIA for AI/VR finance
Spain	Finance	Ministry of Economic Affairs	GDPR + financial compliance	AI-focused; aligned with EU AI Act implementation; 9+ project batches
France	Education/Healthcare	CNIL (data authority)	GDPR (temporary suspensions)	Living-lab approach; discontinued after pilot phase
Finland	Labor Markets	Ministry of Economic Affairs + VTT Research	GDPR (derogations for behavioral data)	34% job placement rate via VR assessments; reduced counselor workload by 40%
Portugal	General (AI/VR/Drones) Tech	National Innovation Agency (ANI)	GDPR	Geographic "Technological Free Zones"; real-world testing enclaves
Italy	Public Services	Presidency of Council of Ministers	GDPR	"Sperimentazione Italia" general-purpose model; limited scalability
Global Models				
South Korea	National Ecosystem VW	Ministry of Science and ICT (MSIT)	PIPA (Korea) + ethical guidelines	World's first <i>Metaverse Industry Promotion Act</i> ;

				\$186M state funding; self-regulation
Singapore	Fintech/Urban Planning	MAS (finance), GovTech (urban)	PDPA (Singapore)	Virtual Singapore 3D digital twin (SGD 73M); MAS sandbox processed 630+ fintech applications
Japan	AR/VR Cross-Sector	Cabinet Secretariat	APPI (Japan)	Permanent cabinet-level sandbox; 30+ approved projects; regulatory reforms (2021)
USA	Medical VR/AR	FDA Digital Health Center of Excellence	HIPAA + UL 8400 safety standard	Streamlined De Novo/510(k) pathways; approved VR medical devices for PTSD/pain
China	State-Led "Practical Metaverse"	Beijing Municipal Government	Strict state control	Anti-speculation policies; €600M+ investment; digital identity systems for user control
UAE	Fintech/VW Finance	ADGM/DFSA Financial Authorities	UAE laws data	<i>Responsible Metaverse Self-Governance Framework</i> ; aligned with Dubai Metaverse Strategy

12 F. METHODOLOGY FOR CASE STUDY SELECTION

Adopted methodology for the execution of the preparatory research to this Policy Brief was structured in three phases, each corresponding to a different and specific objective, namely:

- Phase 1 was aimed at mapping the European state of the art in the domain of regulatory sandboxes, based on published sources
- Phase 2 was aimed at selecting an initial group of case studies, which could be aligned to the general purposes of this research (defining a convenient model to be adopted at the EU level and positively transferred to the Virtual Worlds)
- Phase 3 was aimed to narrow the focus down to a final list of case studies, which are those mentioned in section 3 of this document.

Phase 1 was supported by some preliminary desk analyses and by bibliographic as well as thematic search activities carried out on academic databases, public records on EU and MS websites, and sandbox platform portals.

Phase 2 was supported by discussions and reflections only internal to the team of authors. Adopted selection criteria include, among others: the diversity of legal Regimes, innovation sector, and regulatory maturity.

Phase 3 was supported by face-to-face interviews with 10 external experts, based on a common template.

The three phases have not been connected linearly, but iteratively, as the following drawing exhibits:

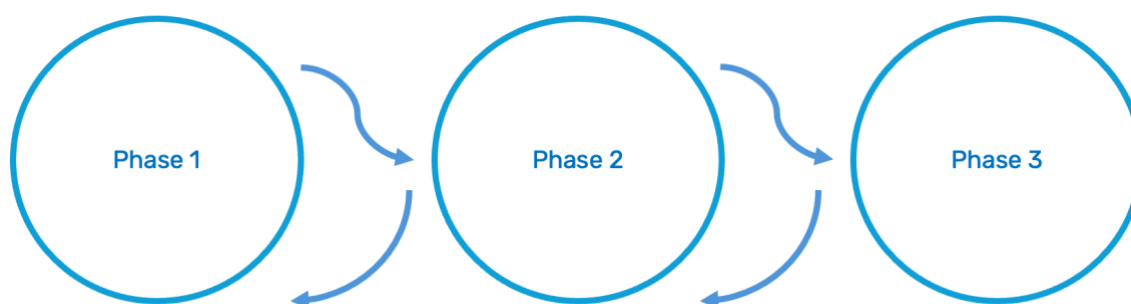


Figure 1. Iterative approach to case study selection

More specifically, the feedback loop from Phase 2 to Phase 1 included additional suggestions for relevant sources to consider in the state-of-the-art analysis; while the feedback loop from Phase 3 to Phase 2 included additional suggestions for case studies to be selected.

Both the state of the art and the selected case studies are described in the following Appendices D and E while Appendix F includes the interview script.

13 G. EUROPEAN STATE OF THE ART

The European policy landscape in regulatory sandboxing for emerging MV/VW related technologies - like virtual reality (VR), augmented reality (AR), artificial intelligence (AI), and Block Chain (BC) - shows a complex picture of evolving frameworks, operational mechanisms, and persistent challenges.

Historically, regulatory sandboxes have been most prevalent and successful in the FinTech sector, where they have facilitated the development and testing of new financial technologies. However, the focus of this research is on the MetaVerse and Virtual Worlds, which present unique regulatory challenges due to their decentralized nature, cross-border operations, novel economic models (e.g., NFTs, cryptocurrencies), and potential societal impacts (e.g., data privacy, digital identity, content moderation, intellectual property, user safety).

Based on an analysis of the case studies presented in Appendix E, which include non-EU Member States like Norway and the United Kingdom, but only represent a minority of EU countries, **three main approaches to regulatory sandboxing** for MV/VW related technologies can be detected:

- **Vertical, or application specific, and nationwide** (e.g. UK, France, Nordic countries);
- **Horizontal, or cross-sectoral, and nationwide** (e.g. Germany, Spain, Portugal and Italy);
- **Vertical, or application specific, and European wide** (e.g. the EU BC Sandbox Initiative).

A common trait to all the approaches is the relative paucity of reusable evidence. This is not limited to the identification of reliable sources – most of which are in fact government's press releases or website pages, including the official texts of normative initiatives – but points at a more substantial lack of information on the outcomes of both the successful and (especially) the unsuccessful pilot projects, including the business and regulatory implications (of the former) and the reasons for failure (of the latter).

We can only speculate about the possible reasons for this scarcity, which may include:

1. Nascent frameworks: the MV/VW are still in their early stages of development, so are the regulatory instruments designed to govern them. Most of the reported sandbox initiatives have only recently been launched, others (not even reported) are in the planning phase.
2. Confidentiality issues: the companies participating in regulatory sandboxes may be hesitant to publicly share detailed information about their applications, especially if they involve proprietary technology or sensitive business strategies.
3. Ongoing pilots: due to the recent emergence of the frameworks, the pilot projects included in the various batches may still be ongoing or not yet finalised up to their impact assessment stage.
4. Reporting delays: even when the case studies are completed, there is often a time lag before their results are evaluated and publicly reported. The process of analysing the implications for regulatory innovation may take even more time and perhaps require additional evidence.
5. Focus on FinTech and AI: the majority of existing regulatory sandboxes are focused on FinTech and, more recently, AI. The application of this model to the MV/VW is a newer development, and it will take time for a body of case studies to emerge.

However, from what can be inferred from the examples provided, the EU MS scenario is characterized by significant heterogeneity and fragmentation. Sandboxes vary considerably in scope, thematic focus, accessibility criteria, operational resources, and governance models. While sectors like healthcare, mobility, and public services are increasingly represented,

financial services remain a dominant theme in many existing national sandbox programs. This scenario (also compared with what non-EU countries such as the United States, China, Japan and South Korea are doing) creates a complex and potentially inefficient environment for innovators seeking to scale solutions across the Single Market and reduces the potential attraction of international investors in EU based SMEs and start up enterprises.

In this scenario, the EU Artificial Intelligence (AI) Act, formally adopted in May 2024, represents a significant driver of acceleration. The Act establishes a risk-based classification system (prohibited, high-risk, limited risk, minimal risk) for AI related technologies, with corresponding obligations for the industrial and non-industrial stakeholders involved in their deployment. A key operational feature mandated by the Act is the creation of regulatory sandboxes in all Member States (Articles 53 & 54). These are intended to provide controlled environments for testing innovative AI systems under regulatory supervision, particularly aiding SMEs and startups in navigating compliance. The Act's provisions are currently undergoing phased implementation, with full application anticipated by mid-2026, as shown in the monitoring overview provided by <https://artificialintelligenceact.eu/ai-regulatory-sandbox-approaches-eu-member-state-overview/>.

Unlike the AI Act, the European Commission's strategy for Virtual Worlds ("An EU initiative on Virtual Worlds: a head start for the next technological transition", COM(2023) 442 final) does not mandate the creation of regulatory sandboxes, but explicitly mentions the experience gained from the EU BC Sandbox Initiative providing a controlled environment for testing innovative AR, VR, AI and BC applications under regulatory supervision, directly feeding learnings back into policymakers.

In fact, a central pillar of the strategy is creating "an enabling environment" for safe experimentation and innovation, as well as to "inform future regulatory and investment decisions". The Council of the EU has endorsed this evidence-gathering role, stressing the need to "identify possible regulatory gaps" (Council Conclusions 9910/24, May 2024, para 15). The key features of the EU BC Initiative, which are likely to be borrowed by the new VW sandbox model, include the following:

- Multi-national Participation: provides a single point of entry for innovators from all over the EU.
- Multi-Regulator Dialogue: facilitates direct engagement between project owners and relevant national and EU-level regulators.
- Focus on EU Legislation: explicitly tests projects against harmonized EU rules (e.g., eIDAS, GDPR, MiCA, DORA) and critical enablers like interoperability and e-Identity.
- Thematic Diversity: projects span sectors including health, supply chain, energy, intellectual property, and public services, demonstrating a broader scope beyond finance.

This represents a practical model for addressing regulatory complexity in cross-border contexts and fostering dialogue on harmonized EU rules.

The exploration of a VW sandbox complements other elements of the EU strategy, such as large-scale industrial pilots (e.g., CitiVerse), the development of standards for interoperability, and skills initiatives like the Academy on Virtual Worlds.

14 H. INITIAL SET OF CASE STUDIES

Below is a selection of 30 real-world case studies—chiefly from Europe but also from overseas—where regulators have set up sandboxes to enable or oversee development and testing of innovative applications. Wherever possible, priority has been given to the identification of cases directly related with MV/VW environments. However, due to the paucity of available evidence, some illustrative examples have also been included from e.g. the Financial Sector (historically the first application domain of the regulatory sandbox concept) or the Block Chain and Digital Ledger Technology (which is indirectly connected with MV/VW, for reasons that are better explained in the entry descriptions).

Each entry lists:

1. Country
2. Location
3. Case owner
4. Application, scope & purpose
5. MV/VW environment
6. Role of the sandbox
7. Success or failure
8. Results
9. Grade (A–D)
10. References

Assigned grades correspond to the following grid:

- A – Well-established, continuously evolving, with proven track record
- B – Successful with caveats or not completely fitting this research purposes
- C – Promising case but not yet implemented, or not fully
- D – Out of scope / interest for the study or evidently unsuccessful

Following is a map of the site locations worldwide:

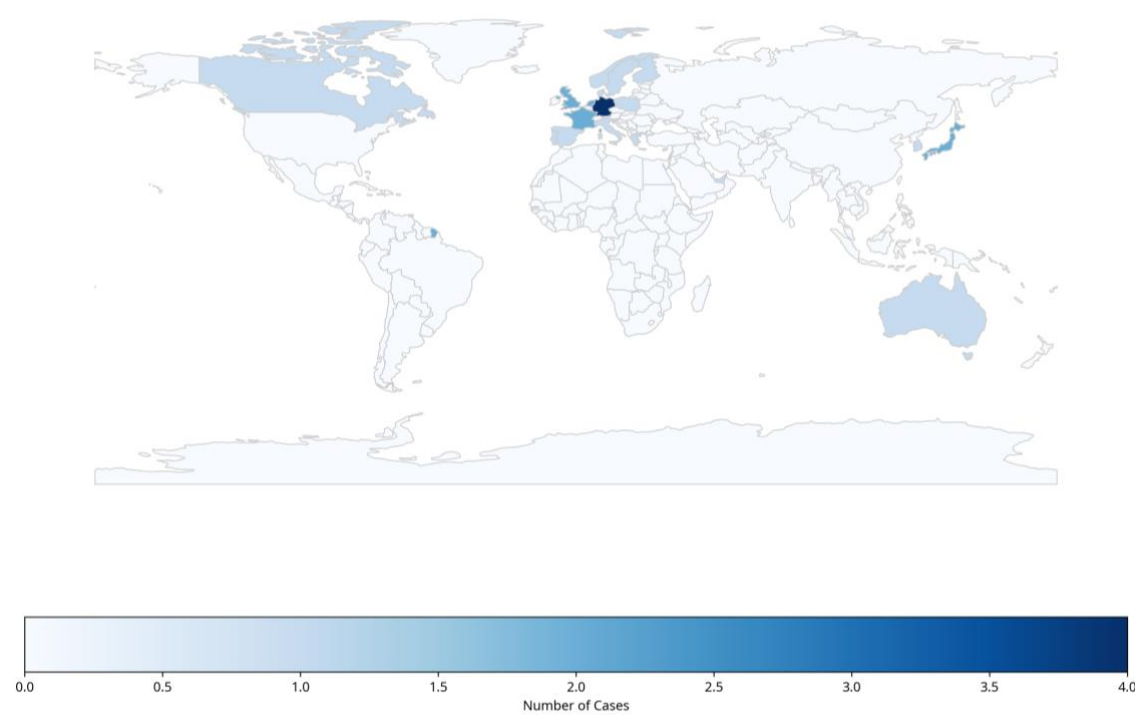


Figure 2. Locations of the selected case studies

E1. United Kingdom — Oxford VR in the MHRA Digital Health Sandbox

1. Country: United Kingdom
2. Location: nationwide (pilot sites across NHS trusts)
3. Case owner: Oxford VR (spin-out from Oxford University)
4. Application, scope & purpose: A clinically validated VR-based cognitive-behavioural therapy (CBT) platform to treat anxiety disorders and phobias. The aim was to demonstrate safety, efficacy and data-protection compliance in real NHS settings.
5. MV/VW environment: Oculus Rift-based 3D virtual environments simulating social situations (e.g. flying, public speaking) for graded exposure therapy.
6. Role of sandbox: MHRA's digital health sandbox granted a temporary waiver from full medical-device certification, allowing iterative trials under regulator supervision.
7. Success or failure: Successful
8. Results obtained:
 - CE marking secured in 2020
 - 75% of patients showed clinical improvement at 6-week follow-up
 - Rapid NHS adoption in 5 trusts by 2022
9. Grade: A
10. References: <https://www.digitalhealth.net/2020/03/nhs-offers-new-virtual-reality-treatment-for-patients-with-social-anxiety/>, <https://www.psy.ox.ac.uk/research/oxford-cognitive-approaches-to-psychosis/projects-1/oxford-virtual-reality-vr-for-mental-health>

E2. United Kingdom — FCA Digital and AI Sandboxes

1. Country: United Kingdom
2. Location: London
3. Case owner: Financial Conduct Authority (FCA)
4. Application, scope & purpose: the FCA operates multiple sandbox programs including a Digital Sandbox (permanent since 2023) and a new "Supercharged Sandbox" launched in partnership with NVIDIA in 2025. While primarily for FinTech, these sandboxes accept applications involving AI, VR, and AR technologies for financial services innovation.
5. MV/VW environment: Financial services applications incorporating VR/AR for banking interfaces, AI-driven advisory services, and immersive financial data visualization.
6. Role of sandbox: Provides regulatory relief, synthetic data access, and controlled testing environment with over 1,000 APIs available. The sandbox allows temporary exemptions from full regulatory compliance while testing innovative products.
7. Success or failure: Successful
8. Results obtained:
 - Over 630 applications received since launch, with continuous expansion of capabilities
 - 40% of participants in fraud detection testing either launched products, secured partnerships, or obtained funding
 - The sandbox has processed applications from distributed ledger technology, AI, and crypto/DeFi companies
9. Grade: A
10. References: <https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms>, <https://www.techmonitor.ai/digital-economy/ai-and-automation/fca-digital-sandbox-financial-services>

E3. France — Virtual Reality in Secondary Education

1. Country: France
2. Location: Paris, various application sites nationwide
3. Case owner: CNIL, Commission Nationale Informatique et Libertés
4. Application, scope & purpose: Pilot use of VR classrooms and immersive learning modules in secondary schools with Living lab/sandbox approach allowed for real-world deployment and feedback.
5. MV/VW environment: VR-based classrooms, collaborative virtual labs for STEM education.
6. Role of sandbox: Temporary regulatory waivers for data protection and curriculum flexibility, adjustments for privacy and educational standards.
7. Success or failure: Successful but probably discontinued
8. Results obtained:
 - A skills portfolio for learners (Daylindo)
 - An exchange tool between the family and the school (Klassroom)
 - Promote and disseminate data from training courses (France Université Numérique)
 - A “personal cloud” for students connected to their digital workspace (Academy of Rennes).
9. Grade: B
10. References: https://www.cnil.fr/sites/cnil/files/2023-07/bilan_bac_a_sable_edtech.pdf

E4. France — Virtual Reality in Healthcare

1. Country: France
2. Location: Paris, various application sites nationwide
3. Case owner: CNIL, Commission Nationale Informatique et Libertés
4. Application, scope & purpose: Developing and testing VR and AR applications for healthcare, including virtual consultations, medical training simulators, and immersive therapy sessions.
5. MV/VW environment: Virtual healthcare platforms and medical training simulators
6. Role of sandbox: Temporary suspension of certain healthcare regulations to test innovative healthcare delivery models and technologies.
7. Success or failure: Successful but probably discontinued
8. Results obtained:
 - Federated learning between several health data warehouses (Lille University Hospital and Inria)
 - A diagnostic aid solution in oncology (Resilience)
 - Anonymous statistical indicators of description of populations in medical research (Clinityx)
 - A therapeutic game for minors with eating disorders (Arras University Hospital).
9. Grade: B
10. References: https://www.cnil.fr/sites/cnil/files/2023-07/bilan_bac_a_sable_sante_numerique.pdf

E5. Netherlands — National Innovation Centre for Privacy-Enhancing Technologies (NICPET)

1. Country: Netherlands
2. Location: The Hague, Nationwide

3. Case owner: TNO (Netherlands Organization for Applied Scientific Research)
4. Application, scope & purpose: A collection of PETs (e.g. Secure Multi-Party Computation, Federated Learning, Synthetic Data Generation) ensuring sensitive personal data is used responsibly when government bodies or agencies are addressing societal issues and challenges.
5. MV/VW environment: None specific. A pilot was set up by TNO with the Social Insurance Bank (SVB) and the Employee Insurance Agency (UWV) within the framework of the Supplementary Provision of Income for the Elderly (Aanvullende Inkomensvoorziening Ouderen, AIO).
6. Role of sandbox: Adoption of Secure Multi-Party Computation exempted SVB officials from certain GDPR data storage and minimisation obligations, as it allows to process data securely without having to access it.
7. Success or failure: Successful but not completely fitting
8. Results obtained:
 - Collaboration with the Dutch Ministry of Home Affairs
 - Collaboration with the Dutch Ministry of Justice and Security
 - Collaboration with the Netherlands Chamber of Commerce
9. Grade: A
10. References: <https://www.tno.nl/en/digital/data-sharing/privacy-enhancing-technologies/>, <https://www.tno.nl/en/newsroom/insights/2023/06/technological-legal-innovation-essential/>, <https://www.tno.nl/en/newsroom/insights/2023/08/authorities-learn-nicpet-seize/>

E6. Netherlands — European Blockchain Sandbox - Digital Product Passports

1. Country: Netherlands
2. Location: The Hague, European Union
3. Case owner: Circularise B.V.
4. Application, scope & purpose: Development and testing of a platform for secure data sharing and traceability across supply chains using blockchain technology. The purpose is to enable companies to comply with increasing regulations (e.g., Ecodesign Directive, Digital Product Passports) by securely sharing sensitive data without exposing intellectual property.
5. MV/VW environment: Block Chain based.
6. Role of sandbox: Participation in the European Blockchain Sandbox provides a structured dialogue with EU and national regulators. This allows Circularise to test its solution against various legislative standards and receive guidance on regulatory compliance, ensuring their technology is flexible enough to adapt to future requirements. It helps in understanding how their secure data sharing mechanisms fit within existing and emerging EU regulations.
7. Success or failure: Probably successful but detailed information is missing
8. Results obtained:
 - The pilot addresses a clear regulatory need (Digital Product Passports) and has implications for trade/industry competitiveness and sustainability
 - The concept of secure data sharing for physical products is based on a 'digital twin'-like representation that can be integrated into future virtual environments for supply chain visualization, product lifecycle management, and consumer interaction.
9. Grade: B

10. References: <https://www.circularise.com/>, <https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/European+Blockchain+Sandbox+announces+the+selected+projects+for+the+second+cohort#EuropeanBlockchainSandboxannouncementtheselectedprojectsforthesecondcohort-CirculariseB.V.>

E7. Germany – Reallabore-Gesetz (BMWK)

1. Country: Germany
2. Location: Nationwide
3. Case owner: Federal Ministry for Economic Affairs and Climate Action (BMWK)
4. Application, scope & purpose: Introduce a national regulatory sandbox framework.
5. MV/VW environment: Not exclusively, but one of the experimentation foci (see below).
6. Role of sandbox: Allow temporary exemptions to test innovations under real-world conditions.
7. Success or failure: Successful and ongoing
8. Results obtained:
 - Wide sectorial and cross-sectorial spread—from autonomous mobility to telemedicine, etc.;
 - Urban examples like Hamburg (public governance twins) and Ahaus (commerce & social digital platforms) illustrate extended use in municipal contexts;
 - Forms like the ARENA2036 Industrial MetaVerse pilot directly intersect with MV/VW technologies, allowing VR/AR factory testing.
9. Grade: A
10. References:

https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Downloads/P/reallabore-regulatory-test-beds.pdf?__blob=publicationFile&v=1

https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Downloads/I/info-reallabore.pdf?__blob=publicationFile&v=4

E8. Germany – Reallabore Program – Industrial MetaVerse Pilot

1. Country: Germany
2. Location: ARENA2036 Innovation Campus, Stuttgart, Baden-Württemberg
3. Case owner: Baden-Württemberg Ministry of Economic Affairs, Labour and Tourism (supported by KIT, IPAI, and Wirtschaftsbetrieb)
4. Application, scope & purpose: A Reallabore pilot in the industrial MetaVerse integrating VR/AR with physical factory operations—aiming to simulate production processes, enhance flexibility, training, and sustainability in real manufacturing environments.
5. MV/VW environment: Mixed industrial MetaVerse environment with VR/AR overlays of real factory spaces within ARENA2036.
6. Role of sandbox: Temporarily waive regulations related to workplace safety, data handling, and equipment certification—allowing live testing of VR/AR integrations in real production contexts.
7. Success or failure: N/A (ongoing)
8. Results obtained:
 - Infrastructure set up with €600 k funding;
 - Real-world AR/VR factory tests underway;
 - Initial observations on efficiency and workforce interaction emerging, but final outcomes pending.

9. Grade: C
10. References: <https://wm.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/foerderprojekt-des-wirtschaftsministeriums-startet-reallabor>

E9. Germany – Reallabore Program – Digital Twin Pilot

1. Country: Germany
2. Location: Hamburg (HafenCity)
3. Case owner: City Science Lab, HafenCity University Hamburg
4. Application, scope & purpose: A Reallabore pilot developing digital twin tools for urban planning and community engagement—to visualize city scenarios and public consultations in VR-like environments.
5. MV/VW environment: Urban virtual twin accessible via web/VR interfaces, replicating city landscapes for simulation.
6. Role of sandbox: Allow experimentation and testing of public participation tools without full compliance obligations with GDPR, to gather public input in near-live virtual models.
7. Success or failure: Successful
8. Results obtained:
 - Ongoing since 2022, with sustained deployment;
 - Enhanced citizen engagement in urban planning;
 - Iterative improvement of the digital twin models;
 - Formal integration into city planning processes reported.
9. Grade: A
10. References: <https://www.frankfurt-university.de/de/newsmodule/pressemitteilungen/reallabore-gesetz-experimentierraume-nachhaltig-und-partizipativ-gestalten/> <https://www.reallabore-innovationsportal.de/reallabore/landkarte.php>

E10. Germany – Reallabore Program – Ecommerce & Social Interaction Pilot

1. Country: Germany
2. Location: Ahaus, North Rhine-Westphalia
3. Case owner: City of Ahaus with private–public sector partners
4. Application, scope & purpose: Creation of a smart commerce and interaction platform blending physical city functions with digital overlays—featuring city-wide app portals, digital vouchers, and virtual marketplaces.
5. MV/VW environment: Mobile/web-based platform with augmented citizen interactions, digital city portal integration.
6. Role of sandbox: Allow regulatory exemptions related to commercial vouchers, data, and digital retail compliance.
7. Success or failure: Successful
8. Results obtained:
 - Ongoing since 1986, with digital enhancement;
 - Numerous functioning services: smart commerce vouchers, 24/7 digital supermarkets, crowd-based mobility apps;
 - Documentation available on the portal.
9. Grade: A

10. References: <https://www.evergabe.de/news/reallabore-gesetz-beschlossen/>
<https://www.bundestag.de/dokumente/textarchiv/2025/kw21-de-reallabore-1075222>
<https://www.reallabore-innovationsportal.de/reallabore/landkarte.php>

E11. Denmark — European Blockchain Sandbox - Real Estate Tokenization

1. Country: Denmark
2. Location: Aalborg, European Union
3. Case owner: DigiShares A/S
4. Application, scope & purpose: Development and testing of Real Estate Exchange, a platform for tokenizing real estate assets and facilitating their trading in the EU. The purpose is to democratize access to real estate investments, enhance liquidity, and streamline processes through blockchain technology. This relates to commerce and financial aspects within a digital asset framework.
5. MV/VW environment: Block Chain based.
6. Role of sandbox: Allows to engage with regulators on the legal and regulatory implications of tokenizing real estate across different EU jurisdictions. This is crucial for ensuring compliance with financial regulations (e.g., MiCA, AML directives), property laws, and investor protection rules, which can vary significantly across Member States. The sandbox helps identify and address regulatory ambiguities and build trust in this novel financial instrument.
7. Success or failure: Probably successful but detailed information is missing
8. Results obtained:
 - The pilot addresses a significant market need for liquidity and accessibility in real estate
 - Regulatory compliant tokenization and trading of real estate assets across the EU can lead to a more efficient and accessible real estate market, with implications for how physical assets are represented and interacted with in digital spaces
 - While primarily focused on real-world asset tokenization, the concept of tokenized real estate can be directly integrated into Virtual Worlds. Users could own fractional shares of real-world properties represented as digital assets within a VW, enabling virtual tours, investment simulations, or even serving as collateral in virtual economies.
9. Grade: B
10. References: <https://digishares.io/>, <https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/European+Blockchain+Sandbox+announces+the+selected+projects+for+the+second+cohort#EuropeanBlockchainSandboxannounceselectedprojectsforthesecondcohort-DigiSharesA/S>

E12. Norway – AI & VR Regulatory Sandbox (Labour Market & Social Services)

1. Country: Norway
2. Location: Nationwide
3. Case owner: Norwegian Data Protection Authority (Datatilsynet)
4. Application, scope & purpose: Use of AI and VR applications in labour market services, including VR-based job interviews and skills assessments for job seekers.
5. MV/VW environment: Virtual job interview platforms, immersive career guidance tools.

6. Role of sandbox: Provide regulatory guidance and temporary waivers for data processing in VR-based labour market services.
7. Success or failure: Successful and ongoing
8. Results obtained:
 - Enhanced privacy practices and regulatory clarity;
 - Improved user experience and data protection in VR job market tools;
 - Contribution to national guidelines.
9. Grade: A
10. References: <https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/>

E13. Finland – Virtual Job Fair Sandbox (Tekiä Project)

1. Country: Finland
2. Location: Häme region
3. Case owner: Ministry of Economic Affairs and Employment + VTT Technical Research Centre of Finland
4. Application, scope & purpose: Test an AI-driven VW job-matching platform for youth (18–30 yrs) with real-time skills assessment.
5. MV/VW environment: Unreal Engine-based custom environment ("TekiäVerse"), accessible via VR and browsers.
6. Role of sandbox: GDPR derogation for processing behavioural data (avatar interactions, voice analytics). Waived mandatory in-person counselling requirements.
7. Success or failure: Successful but scalability challenges in rural areas
8. Results:
 - 11,500+ users (2023–2024);
 - 34% secured jobs/training within 3 months (vs. national average 22%);
 - Reduced counsellor workload by 40%;
 - GDPR-compliant AI framework developed.
9. Grade: B
10. References: <https://www.vttresearch.com/en/news-and-ideas/teki%C3%A4-towards-human-centered-and-trustworthy-ai-public-employment-services>
<https://julkaisut.valtioneuvosto.fi/handle/10024/165406>

E14. Sweden – Virtual Training for Emergency Services

1. Country: Sweden
2. Location: Stockholm
3. Case owner: Swedish Civil Contingencies Agency (MSB)
4. Application, scope & purpose: Development and testing of immersive virtual reality (VR) training simulations for emergency responders (firefighters, police, paramedics). The purpose is to provide realistic, safe, and cost-effective training for high-stress scenarios (e.g., complex rescue operations, disaster response, public order incidents) that are difficult or dangerous to replicate in the real world.
5. MV/VW environment: Highly realistic, physics-enabled VR environments simulating various disaster sites, urban landscapes, and incident scenes. Uses professional-grade VR headsets and haptic feedback suits.
6. Role of sandbox: In close collaboration with technology developers, setting guidelines for data privacy (especially regarding biometric data from VR interactions), operational safety within the simulation, and ensuring the training meets official certification standards.

7. Success or failure: Successful but scalability challenges in rural areas
8. Results obtained:
 - Demonstrated significant improvements in trainee decision-making under pressure compared to traditional methods;
 - Reduced training costs and logistical complexities;
 - Identified new ethical and data privacy considerations for immersive training, leading to the development of internal guidelines;
 - Positive feedback from participants regarding realism and engagement.
9. Grade: A
10. References: <https://flaimsystems.com/blog/blog-5/sweden-validates-vr-fire-fighting-training-using-flaim-trainer-89> <https://www.xvrsim.com/en/news/1870-km-apart-msb-conducts-exams-remotely-with-xvr/>

E15. Poland — European Blockchain Sandbox - Digital Credentials and Identity

1. Country: Poland
2. Location: Warsaw, European Union
3. Case owner: DoxyChain
4. Application, scope & purpose: Development of a platform for issuing and managing digital credentials and verifiable documents, including student portfolios. The purpose is to ensure authenticity and easy verification of documents, reducing fraud and streamlining administrative processes.
5. MV/VW environment: Block Chain based.
6. Role of sandbox: Allows to test the solution against various EU and national regulations concerning digital identity, data privacy (GDPR), electronic signatures (eIDAS), and document authenticity. The sandbox helps in navigating the complex legal landscape of digital trust services across Member States, ensuring the solution is legally compliant and interoperable.
7. Success or failure: Probably successful but detailed information is missing
8. Results obtained:
 - The pilot has direct relevance to education, labour markets (digital CVs), and public governance (e-government services).
 - However, digital credentials and verifiable identity are also foundational to any robust MV/VW environment. Users in Virtual Worlds will need secure and interoperable digital identities to prove their age, qualifications, ownership of assets, or professional status
 - Gaining regulatory clarity and validation for a blockchain-based digital credentialing system can contribute to building a trusted digital infrastructure essential for the future of digital identity in Virtual Worlds
 - DoxyChain's solution could provide the underlying infrastructure for verifiable digital identities and qualifications, enabling trusted interactions, secure transactions, and access to specific virtual spaces or services based on verified attributes.
9. Grade: B
10. References: <https://www.doxychain.com/>, <https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/European+Blockchain+Sandbox+announces+the+selected+projects+for+the+second+cohort#EuropeanBlockchainSandboxannouncestheselectedprojectsforthesecondcohort-Doxychain>

E16. Slovenia — European Blockchain Sandbox - Supply Chain Traceability

1. Country: Slovenia
2. Location: Ljubljana, European Union
3. Case owner: OriginTrail d.o.o.
4. Application, scope & purpose: Development of a decentralized knowledge graph and blockchain-based traceability solutions for supply chains. The purpose is to enhance transparency, trust, and data integrity across complex supply networks, enabling consumers to verify product origins and companies to manage their supply chains more effectively.
5. MV/VW environment: Block Chain based.
6. Role of sandbox: Allows to engage with regulators on the legal and regulatory implications of decentralized data sharing and traceability, particularly concerning data ownership, privacy, and compliance with various industry-specific regulations (e.g., food safety, product labelling). The sandbox helps in validating the legal robustness of the decentralized knowledge graph and ensuring its interoperability with existing regulatory frameworks.
7. Success or failure: Probably successful but detailed information is missing
8. Results obtained:
 - Gaining regulatory clarity and validation for a decentralized supply chain traceability solution that enhances transparency and trust in various industries contributes to building the foundational data layer for future industrial MetaVerse applications
 - While not directly a VW application, the solution's focus on creating verifiable and interconnected data about real-world products and supply chains is a foundational element for an industrial MetaVerse or digital twin environment. This allows for immersive visualization, real-time monitoring, and interaction with digital twins of physical assets within a VW, enabling better decision-making, quality control, and consumer engagement.
9. Grade: B
10. References: <https://origintrail.io/>, <https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/European+Blockchain+Sandbox+announces+the+selected+projects+for+the+second+cohort#EuropeanBlockchainSandboxannounces+the+selected+projects+for+the+second+cohort-OriginTrail>

E17. Italy – General Purpose Regulatory Sandbox

1. Country: Italy
2. Location: Nationwide
3. Case owner: Presidency of the Council of Ministers (Department for Digital Transformation)
4. Application, scope & purpose: “Sperimentazione Italia” (Italy Experiments) is a general-purpose regulatory sandbox open to startups, companies, universities, and research centres. It allows temporary waivers of existing regulations for innovative projects, including those in education, public governance, and social interaction using Virtual Worlds.
5. MV/VW environment: Includes pilots using VR/AR for remote learning, digital public services, and virtual citizen engagement platforms.
6. Role of sandbox: Provides a legal and regulatory safe space for real-world testing of innovations, with temporary suspension of conflicting rules.

7. Success or failure: Successful for public sector and digital transformation pilots, though not all projects are reaching scale
8. Results obtained:
 - Enabled the launch of VR-based remote learning pilots and digital citizen consultation platforms;
 - Produced regulatory learning for future reforms.
9. Grade: C
10. References: <https://iris.luiss.it/retrieve/dc7cd30a-cef5-4190-9c90-f8ecabaec915/8.-Ranchordas-and-Vinci.pdf>

E18. Spain – Regulatory Sandbox in the Financial System

1. Country: Spain
2. Location: Nationwide
3. Case owner: Ministry of Economic Affairs and Digital Transformation
4. Application, scope & purpose: Spain's AI regulatory sandbox is a controlled testing environment that allows innovative technological projects to be implemented in the financial system, fully compliant with the legal and supervisory framework, in order to increase efficiency, service quality, and, particularly, security and protection against new financial technology risks.
5. MV/VW environment: N/A.
6. Role of sandbox: Provide controlled, supervised spaces for testing innovative solutions with tailored regulatory oversight and data protection guidance.
7. Success or failure: Successful, informing broader adoption at the service of the EU AI Act implementation, although not completely aligned with the purposes of this research.
8. Results obtained:
 - Nine batches of supported pilot projects, mostly in the payment system, risk insurance and social security sectors
 - The Spanish law 7/2020 establishes reinforced obligations in the following three areas: (i) the protection of personal data, (ii) the prevention of money laundering and terrorist financing, and (iii) the protection of users of financial services.
9. Grade: A
10. References: <https://dgsfp.mineco.gob.es/es/Sandbox/Paginas/default.aspx>, https://www.tesoro.es/sites/default/files/guia_externa_del_sandbox_enero_2022.pdf, https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2023/20231107_ndp_CMIN%20RD%20Sandbox%20IA.pdf, https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2023/20231003_ndp_Apertura%20prerregistro%20entorno%20de%20pruebas%20IA.pdf

E19. Greece — European Blockchain Sandbox - Secure Digital Communication

1. Country: Greece
2. Location: Athens, European Union
3. Case owner: Konnecta Systems IKE
4. Application, scope & purpose: Development of a secure digital communication platform using blockchain technology, focusing on verifiable interactions and data exchange. The purpose is to provide a trusted environment for sensitive communications, potentially relevant for public governance (secure e-government)

communication), social interaction (private and verifiable messaging), and commerce (secure transaction confirmations).

5. MV/VW environment: Block Chain based.
6. Role of sandbox: Allows to engage with regulators on the legal and regulatory implications of secure, blockchain-based communication, particularly concerning data privacy, electronic identification (eIDAS), and the legal validity of digital interactions. The sandbox helps in ensuring that the platform adheres to EU standards for secure digital communication and data integrity.
7. Success or failure: Probably successful but detailed information is missing.
8. Results obtained:
 - Gaining regulatory clarity and validation for a secure digital communication platform that leverages blockchain for verifiable interactions contributes to building a trusted communication layer essential for various applications within Virtual Worlds, from secure e-governance to private social interactions.
 - Secure and verifiable communication is a fundamental requirement for any interactive MV/VW environment, especially for professional, governmental, or sensitive personal interactions. The solution could underpin secure messaging within virtual meeting spaces, verifiable interactions between avatars representing real individuals or entities, or secure data exchange for transactions in virtual marketplaces. It contributes to building trust and authenticity in digital interactions within the MetaVerse.
9. Grade: B
10. References: <https://konnecta.io/>, <https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/European+Blockchain+Sandbox+announces+the+selected+projects+for+the+second+cohort#EuropeanBlockchainSandboxannouncementtheselectedprojectsforthesecondcohort-KonnectaSystemsIKE>

E20. Portugal – Technological Free Zones

1. Country: Portugal
2. Location: Various application sites nationwide
3. Case owner: National Innovation Agency (ANI - Agência Nacional de Inovação), in collaboration with other entities like the Agency for Administrative Modernization (AMA) and various ministries depending on the sector.
4. Application, scope & purpose: Technological Free Zones are real-world geographical areas where companies can test innovative products, services, and technologies in a live environment with real users for a set period. The primary purpose is to accelerate the transition from experimentation to market-ready solutions by providing a flexible regulatory framework.
5. MV/VW environment: The scope is broad, covering technologies like AI, blockchain, drones, autonomous vehicles, and immersive technologies (AR/VR).
6. Role of sandbox: Provide controlled, supervised spaces, but also technical information, guidelines and recommendations, for testing and experimentation in a real or almost real conditions, with direct and permanent control by the competent regulatory authorities.
7. Success or failure: Successful, but detailed information is missing.
8. Results obtained:
 - Launch of multiple Technological Free Zones in various locations
 - Tested applications include immersive education, smart city management, sustainable mobility, and innovative public governance tools.
9. Grade: B

10. References: <https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/testar-e-incorporar-nova-tecnologia/zonas-livres-tecnologicas-zlt/>

NE1. Singapore — MAS Fintech Regulatory Sandbox

1. Country: Singapore
2. Location: Singapore
3. Case Owner: Monetary Authority of Singapore (MAS)
4. Application, Scope & Purpose: The MAS FinTech Regulatory Sandbox provides a framework for financial institutions and FinTech players to experiment with innovative financial products or services in a live environment, but within a controlled space. The purpose is to foster innovation in the financial sector by allowing for the testing of new technologies and business models that may not fit within existing regulations, while ensuring appropriate safeguards are in place.
5. MV/VW Environment: This regulatory environment encourages innovation in financial services, including those leveraging emerging technologies like Block Chain (BC), Distributed Ledger Technology (DLT), Artificial Intelligence (AI), and virtual assets.
6. Role of the Sandbox: The MAS FinTech Regulatory Sandbox offers applicants a temporary waiver or modification of specific legal or regulatory requirements that might otherwise hinder the testing of innovative solutions. This allows firms to conduct real-world experiments with real customers under close supervision. MAS provides guidance and oversight, enabling them to understand the risks and benefits of new technologies, and to inform future regulatory adjustments. The sandbox aims to strike a balance between promoting innovation and maintaining financial stability and consumer protection.
7. Success or Failure: Successful, although not completely aligned with the purposes of this research.
8. Results obtained:
 - While not a dedicated MetaVerse or Virtual World (MV/VW) sandbox, the MAS FinTech Regulatory Sandbox is highly relevant to the development of MV/VW environments, particularly in the financial services context.
 - It supports the testing of underlying technologies crucial for virtual economies, such as digital payments, tokenization of assets, decentralized finance (DeFi) applications, and identity management solutions that could operate within Virtual Worlds.
 - The MAS Sandbox actively encourages innovation in areas like virtual assets and digital currencies, which are foundational to MV/VW financial ecosystems.
 - The MAS FinTech Regulatory Sandbox has been instrumental in positioning Singapore as a leading global FinTech hub.
 - It has facilitated the testing and eventual launch of numerous innovative financial products and services, attracting both local and international FinTech firms.
 - The introduction of 'Sandbox Plus' further enhanced its flexibility and efficiency, indicating continuous improvement and adaptation.
9. Grade: B
10. References: <https://www.mas.gov.sg/development/FinTech/regulatory-sandbox>, <https://www.mas.gov.sg/development/FinTech/sandbox>

NE2. Singapore — Virtual Singapore Digital Twin & Smart Nation Initiative

1. Country: Singapore

2. Location: Nationwide
3. Case Owner: National Research Foundation (NRF), Singapore Land Authority (SLA), and Government Technology Agency (GovTech)
4. Application, Scope & Purpose: Virtual Singapore is a comprehensive 3D digital twin of the entire city-state, enabling testing and simulation of urban planning scenarios, emergency response procedures, and smart city applications in virtual environments.
5. MV/VW Environment: High-resolution 3D virtual model of Singapore with real-time data integration, allowing immersive exploration and testing of urban scenarios through VR interfaces and digital simulation platforms.
6. Role of the Sandbox: Serves as a living laboratory for testing smart city solutions, urban planning concepts, and public service innovations in a risk-free virtual environment before real-world implementation.
7. Success or failure: Successful, though not exactly a regulatory sandbox.
8. Results obtained:
 - SGD 73 million investment in comprehensive digital twin platform
 - Real-time urban planning and disaster response simulations
 - Enhanced citizen engagement through immersive visualization tools
 - Integration with Smart Nation initiatives and IoT sensor networks
9. Grade: A
10. References: <https://oecd-opsi.org/innovations/virtual-twin-singapore/>, <https://www.tech.gov.sg/technews/5-things-to-know-about-virtual-singapore>, <https://govinsider.asia/intl-en/article/meet-virtual-singapore-citys-3d-digital-twin>, <https://geospatialworld.net/prime/case-study/national-mapping/virtual-singapore-building-a-3d-empowered-smart-nation/>, <https://www.digitaltrends.com/home/virtual-singapore-project-mapping-out-entire-city-in-3d/>

NE3. United Arab Emirates — ADGM RegLab and DIFC FinTech Hive

1. Country: United Arab Emirates (UAE)
2. Location: Abu Dhabi (ADGM) and Dubai (DIFC)
3. Case Owner: UAE's Financial Services Regulatory Authority (FSRA) for ADGM and Dubai Financial Services Authority (DFSA) for DIFC, in collaboration with their respective innovation hubs.
4. Application, Scope & Purpose: The UAE operates multiple regulatory sandboxes, notably the ADGM RegLab and DIFC FinTech Hive, to foster innovation in financial services and emerging technologies. Their purpose is to provide a controlled environment for firms to test new products, services, and business models that leverage technologies like AI, blockchain, distributed ledger technology (DLT), and other FinTech innovations. The scope includes a wide range of financial services, from payments and lending to capital markets and digital assets, with a growing focus on applications relevant to the MetaVerse and digital economy.
5. MV/VW Environment: While not exclusively focused on MV/VW, these sandboxes are crucial for developing underlying technologies (blockchain, AI) that enable MetaVerse applications. The UAE has a broader national strategy, including the Dubai MetaVerse Strategy, to foster a digital economy and attract MetaVerse companies. The sandboxes provide a regulatory testing ground for the financial components and digital asset aspects that would underpin virtual economies within the MetaVerse.
6. Role of the Sandbox: The sandboxes offer a tailored regulatory environment, including waivers or modifications of specific regulatory requirements, for a limited period and with appropriate safeguards. This allows innovators to test their solutions with real customers under close supervision, enabling regulators to gather data,

understand risks, and adapt regulations as needed. They facilitate dialogue between innovators and regulators, promoting legal certainty and responsible innovation.

7. Success or Failure: Successful, although not completely aligned with the purposes of this research.
8. Results obtained:
 - Accelerated development and deployment of innovative FinTech solutions, including Block Chain-based platforms and AI-driven services.
 - Fostered a vibrant ecosystem for startups and established companies in emerging technology sectors.
 - Attracted numerous local and international FinTech firms, contributing significantly to the growth of UAE's digital economy and establishing the country as a global FinTech and innovation hub.
 - Contributed to the UAE's reputation as a forward-thinking jurisdiction for digital innovation.
 - Informed the development of new regulations and frameworks for digital assets and emerging technologies, such as the Responsible MetaVerse Self-governance Framework.
9. Grade: B
10. References: <https://ai.gov.ae/wp-content/uploads/2023/09/Responsible-MetaVerse-Self-governance-Framework-2023-EN.pdf>, <https://u.ae/en/about-the-uae/digital-uae/regulatory-framework/regulatory-sandboxes-in-the-uae>

NE4. Canada — CSA Financial Innovation Hub and Provincial Sandboxes

1. Country: Canada
2. Location: National (Canadian Securities Administrators - CSA) and Provincial (e.g., Alberta)
3. Case Owner: Various regulatory bodies, primarily the Canadian Securities Administrators (CSA) for financial services, and increasingly, provincial governments and federal departments for broader technological innovation.
4. Application, Scope & Purpose: Canada operates regulatory sandboxes primarily to foster innovation in the financial technology (FinTech) sector, including blockchain and digital assets. The purpose is to allow companies to test innovative products, services, and business models that might not fit neatly into existing regulations, under controlled conditions. While not explicitly a 'MetaVerse sandbox', the framework is adaptable to emerging technologies like AI, and discussions are ongoing regarding its application to AR/VR and Virtual Worlds.
5. MV/VW Environment: Direct MetaVerse or Virtual World specific projects within Canadian regulatory sandboxes are less publicly documented compared to FinTech. However, the underlying technologies (Block Chain for digital assets, AI for immersive experiences) are within scope. There is growing interest and research into how privacy laws and regulatory frameworks will apply to immersive technologies (AR/VR/XR) and the MetaVerse, suggesting future sandbox applications in this area.
6. Role of the Sandbox: The regulatory sandboxes provide a 'safe space' for innovators to test new solutions with temporary relief from certain regulatory requirements. This allows regulators to observe the real-world implications of new technologies, identify potential risks, and develop appropriate regulatory responses. They facilitate dialogue between innovators and regulators, aiming to balance innovation with consumer protection and market integrity.

7. Success or Failure: Successful, although not completely aligned with the purposes of this research.
8. Results obtained:
 - Enabled the testing and launch of various Block Chain-based financial products and services.
 - Provided regulatory clarity and pathways for FinTech firms navigating complex securities laws.
 - Contributed to Canada's reputation as a supportive environment for FinTech innovation.
 - Ongoing research and policy discussions are shaping how the sandbox framework will address the unique challenges and opportunities presented by AR/VR and the MetaVerse.
 - Facilitated the entry of several novel financial services into the market. Its adaptability to new technologies like AI and the ongoing discussions around AR/VR/MetaVerse indicate its evolving relevance.
9. Grade: B
10. References: <https://www.canada.ca/en/government/system/laws/developing-improving-federal-regulations/modernizing-regulations/regulatory-sandbox.html>, <https://www.securities-administrators.ca/news/the-canadian-securities-administrators-launches-a-regulatory-sandbox-initiative/>, <https://www.securities-administrators.ca/csa-activities/csa-finhub/>,

NE5. Australia — ASIC's Enhanced Regulatory Sandbox (ERS)

1. Country: Australia
2. Location: National (Australian Securities and Investments Commission - ASIC)
3. Case Owner: Australian Securities and Investments Commission (ASIC)
4. Application, Scope & Purpose: Australia's Enhanced Regulatory Sandbox (ERS), managed by ASIC, allows eligible businesses to test certain innovative financial services and credit activities without first obtaining a license or authorization. The purpose is to facilitate innovation in the financial sector by reducing regulatory barriers for new products and services. The scope includes a broad range of FinTech innovations, including those leveraging blockchain technology, and is increasingly relevant to the underlying infrastructure of digital economies and Virtual Worlds.
5. MV/VW Environment: While the ERS is not a dedicated MetaVerse or Virtual World sandbox, it plays a role in fostering the financial and technological innovations that underpin such environments. Projects involving digital assets, tokenization, and new payment systems, which are integral to virtual economies, can be tested within this framework. Australia is also actively engaged in discussions and policy development regarding the regulation of AI and the MetaVerse, indicating a future-oriented approach to these emerging technologies.
6. Role of the Sandbox: The ERS provides a time-limited exemption from certain licensing and disclosure requirements, allowing businesses to test their offerings with real customers in a controlled environment. ASIC provides guidance and supervision, enabling them to monitor the innovation, assess risks, and inform future regulatory adjustments. This approach aims to strike a balance between promoting innovation and maintaining consumer protection and market integrity.
7. Success or Failure: Successful, although not completely aligned with the purposes of this research.
8. Results obtained:

- Facilitated the testing and market entry of various innovative financial products and services.
 - Provided regulatory clarity and reduced initial compliance burdens for FinTech startups.
 - Contributed to Australia's position as a significant player in the global FinTech landscape.
 - Informed ongoing policy discussions and regulatory responses to emerging technologies like AI and the MetaVerse.
 - The ERS is considered a successful mechanism for fostering FinTech innovation in Australia. It has provided a pathway for numerous companies to test and refine their offerings, contributing to a dynamic financial services sector. Its design allows for adaptation to new technological advancements, including those relevant to the broader digital economy and potential MetaVerse applications.
9. Grade: B
10. References: <https://www.asic.gov.au/for-business-and-companies/innovation-hub/enhanced-regulatory-sandbox-ers/>, <https://www.asic.gov.au/for-business-and-companies/innovation-hub/enhanced-regulatory-sandbox-ers/info-248-enhanced-regulatory-sandbox/>,

NE6. Japan —Regulatory Sandbox System

1. Country: Japan
2. Location: National
3. Case Owner: Government of Japan (Cabinet Secretariat, with various ministries involved)
4. Application, Scope & Purpose: Japan operates a comprehensive Regulatory Sandbox system designed to promote innovation across various sectors by providing a controlled environment for businesses to test new technologies and business models that may not fit within existing regulations. The purpose is to identify and address regulatory barriers to innovation, allowing for the rapid deployment of new services and products. The scope is broad, covering areas such as AI, blockchain, IoT, big data, and other advanced technologies, with an eye towards their application in various industries, including those that could contribute to the MetaVerse.
5. MV/VW Environment: While Japan's Regulatory Sandbox is not exclusively for MetaVerse or Virtual World applications, it is designed to accommodate the testing of underlying technologies that are crucial for their development, such as AI for immersive experiences, Block Chain for digital assets and decentralized identities, and other advanced digital technologies. Japan has a strong interest in the MetaVerse, as evidenced by events like Expo 2025 Osaka MetaVerse Day and various industry initiatives, suggesting that future sandbox projects could directly address MV/VW environments.
6. Role of the Sandbox: The Japanese Regulatory Sandbox allows companies to conduct real-world trials of innovative services or products with temporary exemptions from existing regulations. This enables regulators to observe the impact of these innovations, identify necessary regulatory reforms, and foster a more agile regulatory environment. It aims to balance the promotion of innovation with ensuring safety and consumer protection. The process involves close collaboration between businesses and relevant government ministries.
7. Success or Failure: Successful, although not completely aligned with the purposes of this research.

8. Results Obtained:

- Enabled the testing and implementation of various innovative services and business models that were previously constrained by existing regulations.
- Provided valuable insights for regulatory reform, leading to the amendment or creation of new laws and guidelines.
- Fostered a collaborative environment between the government and private sector to accelerate technological innovation.
- Positioned Japan as a country committed to embracing new technologies and adapting its regulatory landscape accordingly.
- The Japanese Regulatory Sandbox is considered a proactive and successful approach to fostering innovation. It has facilitated numerous projects across diverse sectors, demonstrating the government's commitment to adapting its regulatory framework to technological advancements. Its broad scope allows it to remain relevant as new technologies, including those related to the MetaVerse, emerge.

9. Grade: B

10. References: https://www.cas.go.jp/jp/seisaku/s-portal/regulatorysandbox_e.html,
<https://www.elibrary.imf.org/view/journals/002/2024/116/article-A001-en.xml>,
https://www.jetro.go.jp/en/invest/attractive_sectors/ict/attractive_markets.html

NE7. Japan — Cabinet-Level Regulatory Sandbox for AR/VR

1. Country: Japan
2. Location: Nationwide
3. Case Owner: Government of Japan (Cabinet Secretariat, with various ministries involved, acting as a single point of contact for applicants)
4. Application, Scope & Purpose: Japan's Cabinet-Level Regulatory Sandbox, established in June 2018, is a cross-sectoral initiative designed to test cutting-edge technologies and innovative business models that may not fit within existing regulatory frameworks. Its primary purpose is to enable live testing of new technologies, including AR/VR applications, across diverse industries such as healthcare, mobility, and digital services. The sandbox aims to facilitate regulatory reforms based on real-world data and accelerate the implementation of new technologies into society.
5. MV/VW Environment: The sandbox supports a wide range of AR/VR applications. While specific projects are diverse, they include immersive technologies for medical training, remote assistance, entertainment, and various digital services. The environment is not a single MetaVerse platform but rather a framework that accommodates various AR/VR solutions developed by companies, allowing them to operate under temporary regulatory relief. The focus is on practical applications that can contribute to Japan's economic growth and societal well-being.
6. Role of the Sandbox: The Japanese Regulatory Sandbox provides temporary regulatory relief, allowing businesses to conduct demonstrations and live testing of their innovations under controlled conditions. The Cabinet Secretariat acts as a single point of contact, offering advice, consulting services, and hands-on support to applicants. Competent ministries provide oversight during the testing phase. This framework enables iterative development and facilitates regulatory reform by providing concrete data and insights from real-world trials. The sandbox was initially temporary but was made permanent under the revised Act on Strengthening

Industrial Competitiveness in June 2021, signifying its crucial role in Japan's innovation strategy.

7. Success or failure: Successful
8. Results obtained:
 - Over 30 projects approved across diverse sectors including healthcare, mobility, and digital services
 - Multiple regulatory reforms implemented based on sandbox learnings
 - Permanent framework established under revised Act on Strengthening Industrial Competitiveness in June 2021
 - Cross-ministerial coordination for complex technology testing
 - The sandbox has proven effective in fostering innovation and driving regulatory reform based on real-world data.
9. Grade: A
10. References: https://www.cas.go.jp/jp/seisaku/s-portal/pdf/underlyinglaw/Japans_Regulatory_Sandbox_presentation.pdf, https://www.ey.com/en_jp/services/innovation/regulatory-sandbox-regtech, <https://www.trusted-inc.com/post/japan-s-regulatory-sandbox-empowering-emerging-technologies>

NE8. China — NFT and Block Chain Regulatory Sandbox

1. Country: China
2. Location: Beijing (with similar initiatives in Shanghai and other cities)
3. Case Owner: Beijing Municipal Government (with involvement from various ministries and local authorities)
4. Application, Scope & Purpose: Within the scope of Beijing City's two-year MetaVerse innovation and development plan (2022-2024), the focus is on fostering Web3 technologies, VR/AR applications, and digital identity systems. The plan explicitly mentions exploring regulatory approaches for blockchain and NFT technologies. The overarching purpose is to drive the development of the digital economy, integrate immersive technologies into various sectors, and establish Beijing as a benchmark city for digital innovation, all while maintaining strict government oversight and preventing financial speculation.
5. MV/VW Environment: Government-backed MetaVerse development emphasises practical applications in sectors like digital education, cultural tourism, and urban digital twin applications. This involves the integration of technologies such as 3D visualization and Geographic Information Systems (GIS) to build visual urban spaces and intelligent infrastructure. While fostering these immersive environments, there is a strong emphasis on maintaining strict control over financial aspects of digital assets and user anonymity, differentiating it from more open, decentralized MetaVerse visions.
6. Role of the Sandbox: China's approach to a "regulatory sandbox" for NFT and blockchain technologies within its MetaVerse plan is distinct from typical Western models that grant temporary regulatory exemptions. Instead, it functions more as a framework for 'exploring' and 'guiding' the development of NFT technology trends and blockchain applications under strict government oversight. The goal is to prevent "excessive speculation" in virtual assets and ensure that technological development aligns with national policy objectives, rather than relaxing existing regulations. It's a controlled environment for understanding and shaping the regulatory landscape for these emerging technologies.

7. Success or Failure: Successful but with significant regulatory constraints remaining operational
8. Results obtained:
 - Beijing's plan aiming to drive over €600 million in MetaVerse-related investments across Chinese cities
 - Digital identity system proposals for MetaVerse user control being explored
 - AR/VR technologies being actively integrated in the education and cultural tourism sectors, expanding intelligent and interactive online experiences
 - First national-level Virtual Reality Development action plan released, demonstrating China's strategic commitment to advancing immersive technologies.
9. Grade: A
10. References: <https://cointelegraph.com/news/beijing-announces-two-year-MetaVerse-innovation-and-development-plan>, <https://identityweek.net/china-invested-in-regulation-around-MetaVerse-opportunity/>, <https://www.theblock.co/post/165522/beijing-lays-out-plan-for-MetaVerse-development-in-tech-development-zones>, <https://forkast.news/beijing-releases-web3-white-paper-highlights-challenges-in-talent-rules/>

NE9. South Korea — MetaVerse Industry Promotion Act and AR/VR Innovation Framework

1. Country: South Korea
2. Location: Nationwide
3. Case Owner: Ministry of Science and ICT (MSIT)
4. Application, Scope & Purpose: World's first dedicated MetaVerse industry promotion law, establishing comprehensive regulatory framework for VR/AR technologies, digital identity systems, and Virtual World governance to foster systematic industry development.
5. MV/VW Environment: South Korea is actively building a National MetaVerse ecosystem including VR platforms, AR applications, and Block Chain-based Virtual Worlds. The government has allocated substantial funds (e.g., ₩223.7 billion or approximately \$186.7 million in 2023) to support the creation of MetaVerse platforms, content, and the integration of XR (Extended Reality, encompassing AR/VR) technology into key sectors like education, retail, healthcare, manufacturing, construction, and defence.
6. Role of the Sandbox: While not a traditional regulatory sandbox with explicit waivers for specific companies, South Korea's approach provides a systematic policy framework that functions similarly to a sandbox for the entire industry. The MetaVerse Industry Promotion Act introduces "Provisional Regulatory Guidelines" to address regulatory uncertainties and promote proactive regulatory improvements. It also establishes a legal basis for self-regulation led by the private sector, allowing the industry to proactively address new user protection issues without stifling innovation. This framework provides regulatory guidance and a supportive environment for testing MetaVerse innovations while ensuring user protection and industry growth.
7. Success or failure: Successful
8. Results obtained:
 - World's first MetaVerse industry promotion law enacted
 - \$186.7 million government investment in Virtual World platforms
 - AR/VR intellectual property protection framework established

- MetaVerse ethical principles and user protection guidelines developed
 - Creation of a MetaVerse policy review committee
 - South Korea's proactive and comprehensive approach to MetaVerse development, including dedicated legislation and significant government investment, has positioned it as a global leader in this emerging field.
9. Grade: A
10. References: <https://dailycoin.com/south-korea-is-preparing-MetaVerse-industry-promotion-law/>, <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&bbsSeqNo=42&nttSeqNo=1032>, <https://cointelegraph.com/news/south-korea-expands-its-efforts-to-regulate-MetaVerse>, <https://www.theinvestor.co.kr/article/2710346>, <https://www.seoulz.com/the-ar-and-vr-industry-in-south-korea-a-complete-breakdown/>

NE10. United States — FDA Digital Health Center of Excellence

1. Country: United States
2. Location: Nationwide
3. Case Owner: U.S. Food and Drug Administration (FDA), specifically through its Digital Health Center of Excellence (DHCoE)
4. Application, Scope & Purpose: The FDA's DHCoE plays a pivotal role in the oversight and advancement of digital health technologies, including Virtual Reality (VR) and Augmented Reality (AR) medical devices and digital therapeutics. Its primary purpose is to streamline the regulatory pathways for these innovative technologies, ensuring their safety, effectiveness, and quality for clinical applications. The scope covers a wide range of uses, from diagnosis and treatment to rehabilitation and disease management, across various medical specialties.
5. MV/VW Environment: The DHCoE addresses medical applications within immersive environments. This includes the use of VR platforms for the treatment of anxiety disorders, Post-Traumatic Stress Disorder (PTSD), chronic pain management, and neurological rehabilitation. It also encompasses AR applications for surgical planning, guidance, and training simulations. These technologies often utilize FDA-cleared or approved headsets and software platforms designed for specific medical indications.
6. Role of the Sandbox: The FDA's approach, particularly through the DHCoE, functions as a form of regulatory sandbox by providing a more agile and supportive environment for the development and review of novel digital health technologies. While not a traditional 'sandbox' with explicit waivers, the DHCoE offers clear regulatory guidance, participates in pre-submission discussions, and facilitates expedited review pathways (e.g., through the De Novo classification process or 510(k) clearance) for AR/VR medical devices. This allows companies to test and refine their innovative solutions under the FDA's oversight before full market authorization, fostering innovation while maintaining rigorous safety and efficacy standards.
7. Success or Failure: Successful
8. Results obtained:
 - Multiple VR medical devices received FDA clearance/approval
 - Established clear regulatory pathways for immersive medical technologies
 - Enhanced safety standards for AR/VR medical applications
 - Collaboration with Industry and Standards Bodies
 - UL 8400 safety standard adopted by OSHA for VR/AR equipment
9. Grade: A

10. References: <https://www.fda.gov/medical-devices/digital-health-center-excellence>,
<https://www.fda.gov/medical-devices/digital-health-center-excellence/augmented-reality-and-virtual-reality-medical-devices>,
<https://www.mofo.com/resources/insights/240830-immersive-technologies-the-uncertain-regulatory-landscape>, <https://www.ul.com/insights/osha-adds-ul-8400-nrtl-programs-list-safety-standards>, <https://incompliancemag.com/list-of-medical-devices-incorporating-virtual-reality-technology-updated/>

15 I. EXPERT INTERVIEW SCRIPT

For internal use only, please provide below the information about the interviewer and interviewees. Information about interviewees is only for internal use.

Name and role of interviewee	
Name of organisation of affiliation	
Name of interviewer and date	

F1. Introduction

These guidelines are structured in two parts.

The first part (starting here) provides to the **interviewer**:

- 1) An overview of the purposes of the interview and the way it should be conducted
- 2) Some background notes and the list of questions to be made
- 3) Suggestions for reporting back to the author of the policy brief

The second part (starting on page 5) provides to the **interviewee**:

- 4) An information sheet, to be read and kept
- 5) A consent form, to be signed and returned to the interviewer.

F2. First Part

1. Purposes of the interviews and how they should be conducted

You know that the OpenVerse consortium is engaged in the preparation of a policy brief entitled: *Regulatory Sandboxes for Virtual Worlds Innovation: A Framework for EU Leadership*. It is available here: This link will be shared with the interviewees, although we cannot predict if people will spend their time in reading it before the interview, particularly in case of a too short notice.

The planned interviews, which can be run online and (audio/video) recorded to facilitate transcription, should be done in the following order: first, a small control group belonging to the OpenVerse consortium; then, a selected number (about 10-20) of European stakeholders, chosen from a previous list of 40-50.

In the following we will provide you with some background notes and the list of questions to be made. Then in this same document you can find an information sheet and an informed consent form. Ideally you might start reading the information sheet (or summarising its content) and then get the informed consent form signed. Or you can postpone this till after the end of the interview. This can especially be done in case you decide to record it, as the interviewee may be interested in receiving the transcript in return for the signed form.

Then our suggestion is to read the background notes and only later start with the questions. Timewise, we consider 1 hour (brutto) as global requirement, all included, corresponding to the most frequent duration of a Zoom or Teams session. Therefore, you might want to allocate 5' to the introduction, 10' to the reading of the information sheet and background notes, 40' to the Q&A and 5' to the closure of the interview. These are all indicative times of course.

During the dialogue, you should ensure that the discussion remains on the point and that enough time is allocated to all questions. This is also why you might want to check the timing of your own interview first! And the internal control group can also serve that purpose.

In selecting the interviewees, it is important to ensure gender balance and a certain variety of geographical locations. Re stakeholder types, there should be a different set of profiles, including businesspeople, policy makers, IT experts and lawyers, in order to diversify the inputs

and suggestions received. However, it should be borne in mind that by no means, can the panel of interviewees be considered statistically representative in any respect.

During the Q&A phase, you should make sure that they provide practical insights and actionable recommendations to improve the current version of the policy brief, which we (as OpenVerse consortium) can take stock of in our next and final project phase.

As we cannot rely on the interviewees to have read the document in-depth, please be aware that their replies can only be based on the questions made.

2. Background notes and list of questions to be made

Key Take-Aways

Regulatory sandboxes are controlled environments in which innovators can test products, services, and business models under a regulator's oversight. The goals include fostering experimentation, collecting evidence for future policymaking, and building dialogue between regulators and industry.

This OpenVerse Policy Brief explores the potential of regulatory sandboxes to offer a dynamic, adaptive, and risk-managed framework for balancing innovation with the protection of fundamental rights in Virtual Worlds (VW). As immersive digital environments—from MetaVerse (MV) platforms to Augmented and Virtual Reality (AR/VR) applications, from Blockchain-based ecosystems to Artificial Intelligence (AI)-driven models and simulations—expand in complexity and societal relevance, sandboxes emerge as a crucial, and partly unexplored, regulatory tool.

Rigid regulation can stifle progress; unregulated innovation can harm users. Sandboxes offer a third way—facilitating agile, iterative governance where experimental technologies are monitored in real-time, allowing policy to evolve alongside innovation. This doesn't come without its own complexities, which are not merely extensions of traditional Internet governance issues; rather, they are compounded by the immersive, persistent, and often decentralized nature of VW environments.

Despite the growing interest in regulating innovation in Virtual Worlds, there is a significant lack of detailed case studies around the world, matching the variety of potential, as well as actual, business applications – which range from financial to labour markets, from education to commerce, and from social interaction to public governance. If one broadens the scope to generic (i.e. not specifically oriented to VW) regulatory sandboxes, then the evidence at hand increases in quantitative terms, but the key issue remains unattended of which unavoidable characters of a sandbox environment should be associated with its utilisation for VW innovation.

Another notable gap in the public record is the absence of detailed case studies on unsuccessful sandbox projects, particularly in the MV/VW domain. While some projects may not proceed past the application stage, and others may pivot or fail within the sandbox, the reasons for these outcomes are rarely publicized. This lack of transparency makes it difficult to draw lessons from failure, which can be just as valuable as celebrating success.

Finally, this document draws the distinction between single-country and multi-country regulatory sandboxes. While the former ones serve their purpose in fostering localized innovation, the global and interconnected nature of MetaVerse and Virtual Worlds industries demands a more expansive approach, which should facilitate the temporary lifting or harmonization of complex cross-border rules, thus foster the development of systemic solutions that cut across multiple jurisdictions.

Urgency

Over the past few years, the European Union (EU) has been building a coherent, future-proof framework to govern Virtual Worlds across its Member States. However, it still lacks a cohesive, VW-specific legislative package.

This Policy Brief outlines the scope and functioning of a regulatory sandboxing scheme specifically designed for new European startups and micro-enterprises operating in the MV/VW industries. The scheme is conceptualized around the principles and constitutive features of the

so-called '28th Regime,' an emerging legal framework aimed at fostering innovation and simplifying cross-border operations within the EU.

By institutionalizing sandboxes as a governance tool, the EU can navigate the complexities of Virtual Worlds with foresight and flexibility. Through harmonized action, stakeholder engagement, and global leadership, Europe can help ensure that the digital future remains not only innovative—but fair, inclusive, and democratic.

However, it is necessary to act swiftly to shape the normative and regulatory frameworks that will govern Virtual Worlds. Global competitors are already setting de facto standards. Delayed action risks diminishing the EU's digital sovereignty, innovation leadership, and influence in global tech governance.

Expected readership

Interested readers of this Policy Brief may include EU, national and regional/urban policymakers and legislators/regulators, MV/VW industry stakeholders, investors and the financial community, standardisation experts, researchers, academics and advisors, legal practitioners and IT consultants, civil society and user-rights activists.

This is where our interview starts.

Q1. Personal Knowledge and Experience of Virtual Worlds

Let's start with your own knowledge and experience of the MetaVerse/Virtual Worlds topic. Can you explain your connection with that domain? Make any example you are familiar with?

.....

.....

.....

.....

.....

Q2. Opinion on Virtual World Industries in Europe and abroad

What is your opinion on the development and competitiveness levels of the MV/VW industries in your country and/or at the European level? Think of applications of 3D, AR/VR, Blockchain, Games, etc. - but not limited to them. How do we stand against global competition and why?

.....

.....

.....

.....

.....

Q3. Combining MV/VW Innovation with Regulatory Sandboxing

One of the main arguments of the OpenVerse Policy Brief you have with you in a draft version, is that by extensively adopting the instrument of Regulatory Sandboxes, it would become easier for EU Member States and Europe as a whole to promote and facilitate innovation in MV/VW industries and applications. Do you agree with that argument and why? (Disagreements are welcome). Which aspects of the Regulatory Sandbox instrument you see most useful/appropriate to the purpose, or maybe the least?

.....

.....

.....

.....

.....

Q4. A 28th Regime for the EU MV/VW Innovators

Another main argument of the OpenVerse Policy Brief is that the EU might want to adopt a VW-specific legislative package introducing a regulatory sandboxing scheme specifically designed for new European startups and micro-enterprises operating in the MV/VW industries, modelled as suggested for the so-called ‘28th Regime’ for innovators at an EU scale. Do you agree or disagree with this proposal and why? Any suggestion or recommendation will be welcome.

.....

.....

.....

.....

.....

.....

Q5. (Optional) Additional Inputs

Is there anything else you would like to add about how we could boost the MV/VW industry and market in your country as well as at the EU level?

.....

.....

.....

.....

.....

.....

End of the interview

3. Suggestions for reporting back to the author of the policy brief

After each interview, you are kindly asked to prepare a written transcript in English. We don’t mind whether the interview was recorded or not, or if the transcript was done using AI or not. What matters for us is that the transcript can be used, not in association with the identity of the respondent (that is not part of the purpose – quite the contrary, received replies need to be anonymised before publication) but to improve the depth and robustness of the results we are generating with this Policy Brief.



Information sheet

Thank you for agreeing to take part in this EU-funded Horizon Europe Coordination and Support Action, OpenVerse, which aims to create inclusive, open, and ethically responsible Virtual Worlds, thus enhancing the EU's technological sovereignty in the global arena. For more information and details of the Action's aims, partners and activities, please visit our official website: <https://open-verse.eu>.

Before we continue with the interview, it is important that you understand why and how this research is being carried out and what your involvement in it will be. Please take time to read the following information carefully and discuss it with others if you so wish.

If there is anything that remains clear or if you would like to receive more information, send an email to the lead author of the Policy Brief, Francesco Molinari, Senior expert at The Lisbon Council (francesco.molinari@lisboncouncil.net).

Take time to decide whether you want to participate or not.

Thank you for reading this information sheet.

1. Interview purpose

OpenVerse and particularly its coordinator, The Lisbon Council, is in the process of drafting a Policy Brief entitled "Regulatory Sandboxes for Virtual Worlds Innovation: A Framework for EU Leadership". You have/have not been shared the contents of the draft that is currently under embargo for reasons of business confidentiality.

To validate the draft contents, we are now conducting interviews with some domain experts and that is why we contacted you.

2. Data gathering (including your personal data)

We have prepared a set of questions and would like to make audio/video recordings for accuracy. Each interview lasts approximately one hour. It will be conducted in English, using mainly online tools (e.g., Zoom, Microsoft Teams).

Our conversation will then be recorded and transcribed, i.e., written down according to certain rules, and we will compare the answers with those of other experts to get an overview of the prevalent opinions of respondents.

We may contact you again for a follow-up meeting to discuss and enrich the findings from the initial data analysis.

3. Processing (and confidential treatment if personal) of the information gathered

For internal usage, the research team will pseudonymize personal data. To achieve this, we will keep a list with personal data separate from the interview data and we will assign an alphabetical code to each organisation and a numerical code to each interviewee (e.g. A-01).

For external usage (i.e., project reports, conference meetings, scientific publications, university lectures) the results will only be used in an aggregate form.

Confidentiality will be maintained through the following actions:

- The name-code pairs will be stored on secure password-protected computers, connected to the internet. Only authorized project staff will have access to them.
- For all other data stored on the partner organizations' servers, partners will make sure that appropriate security measures are in place.
- Raw data (including audio/video recordings) will be destroyed 5 years after the project has ended.
- Data will be used only for research purposes (scientific papers, academic and project related conferences, lectures etc.).
- No results will be presented in any way that can reveal the identity of a single person or group of respondents.
- Commercial uses of the data are not permitted and no one outside the project will be allowed access to the original recordings.
- Legal access to the data from outside is not possible.

4. Analysis of interview data

We will analyse the interview transcripts, including, if necessary, by the use of state-of-the-art AI and statistical tools, and generate aggregate reports of the received responses, to protect the anonymity of the interviewees in full.

Some sentences of particular relevance to characterise or summarise the prevalent opinion of a respondent, may be captured *verbatim*, i.e. as a faithful reproduction, using inverted commas, but never disclosing the identity of the person.

Globally the transcripts will be used to identify the high-ticket items and validate, or disqualify, the contents of the current Policy Brief draft.

5. Your rights

It is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep and asked to sign a consent form.

You can withdraw at any time from the interview without giving a reason and without affecting any benefits to which you are entitled.

6. Benefits and risks of taking part in the project

There are no direct benefits for you as a person if you participate in this interview. However, there can be some indirect benefits from influencing, with your opinions, the future course of the EU policy making in the area.

We do not envisage any psychological, social, economic or other risk to respondents taking part in the interview.

We will manage the whole process in accordance with the GDPR – the EU General Data Protection Regulation.

CONSENT TO PARTICIPATE IN A COORDINATION AND SUPPORT ACTION ("OPENVERSE")

FUNDED BY THE EUROPEAN COMMISSION

Declaration of consent

- I the undersigned, have read and/or had the preceding Information Sheet read and/or explained to me and fully understood its contents.
- I was informed by the interviewer about the interview purposes and the mechanisms of data collection and processing and all my questions were answered comprehensively and satisfactorily.
- The benefits and possible implications of my participation in this research have been explained to me in full and I understand that there are no foreseeable risks involved.
- I was informed that the interview may/shall be recorded.
- I know that my personal data will be pseudonymized and only processed in an aggregate form.
- I am aware that all information collected is stored and processed on secure password-protected computers, connected to the Internet, and that all authorized project staff who have access to that information are subject to confidentiality.
- I am aware that my personal data will never be shared with anyone else than the project partners listed in the Information sheet.
- I am accepting to be interviewed voluntarily and know that I can withdraw at any time.

Place and date: _____

Name and surname: _____

Signature: _____

16 J. SELECTED FEEDBACK RECEIVED FROM INTERVIEWED EXPERTS

Question #2 – What is your opinion on the development and competitiveness levels of the MV/VW industries in your country and/or at the European level? Think of applications of 3D, AR/VR, Blockchain, Games, etc. - but not limited to them. How do we stand against global competition and why?

“I think that we are really creative in the different technologies that enable this immersive world. And this is a strength. And even we are also scientifically very good. But I think we are a bit fragmented (...) And we lack also, I think, the capacity to scale up”. (C. Barelle)

“Access to capital, it's a big aspect, no? And also, I would say, let me think. Yeah, I would say access to capital and maybe also a little bit of language fragmentation”. (E. Ferro)

“On the legal side, I think there's an issue of the precautionary nature of the European environment compared to that of the American, Chinese, or African environment. We, in the absence of doubt, won't take the risk (...) For me, a big problem is more about thinking, culture, than about the law itself”. (G. Colclough)

“I think all of us are aware that the European Union, from a perspective of regulation, the development of artificial intelligence in comparison to, for example, China or in the United States. That doesn't mean it's a bad thing, but from a competitive perspective, it definitely holds us back”. (K. Le Moignic)

“I like to compare Europe to a middle-aged man. He's comfortable in his life, he's comfortable, and all is well, let's not rock the boat. But if we don't look to the younger generation, to the more resilient generation, like in Ukraine, and say that we have to fight as an association, because we have pride in an open economy”. (G. Corbett)

“For me, as an innovation focused on decentralization in this matter of infrastructural sovereignty, I think Europe is a pioneer. Specifically in Spain, I think we have a lot of industry, a lot of potential. We're at the forefront of advanced digital skills; we're among the first in Europe (...) However, if we talk more about the virtual worlds themselves, I think we're a little behind”. (E. Alvarez Corona)

“My theory is that this has a lot to do with Europe not having a cohesive visual culture (...) Nonetheless, we share a very similar ethos, which we can trace back to humanism, or even the democratic and republican values of the French Revolution. (...) I think that in the visual community, that's like a barrier we have, because those things that are seen as attractive in Spain, I don't know, in northern Europe are seen as invasive or too extravagant”. (E. Alvarez Corona)

“It was also bad timing (for virtual worlds) because you have to triangulate this with the end of the pandemic”. (E. Alvarez Corona)

“Being so many countries, each one of a few special characteristics, we are very slow to regulate. And that, well, it is true that it hinders us a lot in terms of innovation (...) Technology advances at an abysmal speed and regulations, obviously not. It is regulated when you see the things that happen. That is obvious, it is always regulated from behind. Here it is easier to capture investment and everything else, so I understand that the main engine of these decisions may be investment, but surely regulation and also the tax burden at the tax level also has something to do with it”. (P. Vela)

“For sure, we have a very complex regulatory framework ... The regulatory framework kind of inhibits innovation”. (T. Papaioannou)

“Virtual worlds in the old sense, meaning the gaming industry, we're doing extremely well. We're world leaders in that space, so that I think is where we shine (...) When it comes to cloud, cloud services, cloud infrastructure, we're massively lagging behind. It appears to be very difficult to pick up pace. I think we all know that at least there's a perception, but I think there's a truth in it, that our legislation tends to stifle a bit through innovation. These laws are very abstract in the terminology and the rules that they introduce, because there is this clear goal of being technologically neutral (...) It's only after an authority has come up with a case or a court has come up with a judgment that you know for sure how you have to interpret it. So, guidance comes too late. Guidance is too detailed, is too fragmented”. (R. Roex)

Question #3 - One of the main arguments of the OpenVerse Policy Brief you have with you in a draft version, is that by extensively adopting the instrument of Regulatory Sandboxes, it would become easier for EU Member States and Europe as a whole to promote and facilitate innovation in MV/VW industries and applications. Do you agree with that argument and why? (Disagreements are welcome). Which aspects of the Regulatory Sandbox instrument you see most useful/appropriate to the purpose, or maybe the least?

“Virtual world is a wrapper about activities that happen in the world, okay? (...) So, the question is, do they create something new that was not present before that needs to be regulated or not?”. (E. Ferro)

“The idea is, let's say, in a virtual, though non-physical, space, this regulatory regime, right?... One would be specific to virtual worlds, which is a particular type of digital business, where there is... it's very dynamic, it's like AI, it changes every month, the tools you had a few months ago are different”. (G. Colclough)

“If we take a regulatory sandbox as a controlled environment where companies can test products, services and models under regulatory conditions, and this extends to a remote space without needing what we would call a full physical development, I think that's quite ... I think it's very good. The issue is who has access, right? And how is it accessed? And that's the real question of how... Who would ultimately have a say in these regulatory virtual worlds. Who has access. And I think that's really my biggest criticism”. (E. Alvarez Corona)

“I associate a sandbox or a virtual world a lot, something where I have a purpose and I can move freely or have free decision power. When we talk about a regulatory sandbox, it is hard for me to see it because I understand that a regulatory sandbox is a place where you can apply regulations and see how they affect users, but I don't see that as a user. It is not easily visualized, right?”. (P. Vela)

“I think that there is a lack of integration of the virtual worlds into the real worlds and a lack of nice use cases ... Right now it's something like which is totally artificial, totally isolated from the real world. So yeah, I think this connection is missing. For testing ideas in a safe environment, this could be a very interesting idea (...) Any items exchange in this virtual world could emerge without any kind of risks”. (T. Papaioannou)

“I don't know, or at least I'm not convinced, whether the virtual world layer adds much. I would still be processing personal data. So, GDPR would still apply. That means involvement of the supervisory authority to avoid it, but the authorities have no resources. So, how does the virtual world resolve it? That's what I don't see”. (R. Roex)

“The risks to manage here are fragmentation (many different sandbox rules does not solve the problem; recreates it); regulatory arbitrage and softening protections (which is particularly tricky in the consumer market sphere and with regard to successful content offer, which is difficult to control once released) and capacity asymmetry, since smaller NCAs may struggle to supervise complex VW pilots (biometrics, payments, IP)”. (J.M. Aguado)

Question #4 – Another main argument of the OpenVerse Policy Brief is that the EU might want to adopt a VW-specific legislative package introducing a regulatory sandboxing scheme specifically designed for new European startups and micro-enterprises operating in the MV/VW industries, modelled as suggested for the so-called ‘28th Regime’ for innovators at an EU scale. Do you agree or disagree with this proposal and why? Any suggestion or recommendation will be welcome.

“I think that the innovation is coming from the startup, actually, and not that much, and we can see it in Ontochain or in TrustChain, and not that much from a big company, at least in Europe”. (C. Barelle)

“The 28th regime should be considered as a minimum common denominator in terms of rules. So, you should not add on top what is existing there. So, we should strip all the, let's say, unnecessary regulations and say, okay, this is the core”. (E. Ferro)

“The first question of any Ukrainian company, majority or community, which would be: is it in line with Europe? Has Europe approved this? Because there's a lot of work in terms of getting the various chapters of the acquis and moving towards the European Union hopefully by 2030 (...) The access to Europe is extremely important for Ukraine, whether economically, politically or symbolically. It's the strategic north star of everything that's happening”. (K. Le Moignic)

“I think also the issue of digital skills and digital literacy... Of course. The space that civil society has in this, right? Civil society, third-sector actors, and also public-sector actors. I think it's good, really. I think it's a very good idea (...) I think it will help us not to have that burden, as I told you at the beginning, of worrying about each of the 27 national laws that make up the entire European ecosystem”. (P. Vela)

“If they want to expand across the European continent, they would have to go looking at each step they take, if they are complying with the regulation or not, they would have to contact an expert, they would have to do an internal audit for each of the steps they want to take, and I think doing this 28th regime makes it easier to do it all at once”. (P. Vela)

“It's an interesting idea. It's an interesting idea, especially as a testbed for new ideas that may be applied later at the real world”. (T. Papaioannou)

“In principle, the 28th regime is exactly the kind of tool that could give European VW builders a single-entry point to test and scale across the EU (...) the 28th Regime might become a backdoor to weaker labour and consumer protection, which is a sensitive issue in the context of platform economy”. (J.M. Aguado)

Status of validation of the policy brief

“I think it's a very good idea. And I agree that it can play a big role in accelerating the innovation. The barrier, I think, we have to be careful once again to fragmentation”. (C. Barelle)

“At some point, the startup or the SMEs will have to scale up in Europe and will have to comply with the regulations. So, if by design all the constraints are already taken into consideration

and the solution is tested in this kind of environment, I think it will be a big support for them to scale up easily". (C. Barelle)

*"We need to support industry across Europe. We don't compete with each other. We are a continent. We are a union. We need to compete together against the others
I think we need something that with one action allows you to operate in a single market, in a single European market, okay? So, we need the 28th regime. What I'm saying is that the 28th regime needs to be lean and fast". (E. Ferro)*

"Small businesses and SMEs are an important lifeblood for Europe... What we need to do is to create an environment that, in my opinion, works well beyond a policy context". (G. Colclough)

"If we take a regulatory sandbox as a controlled environment where companies can test products, services and models under regulatory conditions, and this extends to a remote space without needing what we would call a full physical development, I think that's quite interesting." (K. Le Moignic)

"However, when we look at it in terms of citizen issues, there are... I have my doubts. Because what you're thinking is that very large companies could end up having influence over how all this plays out". (E. Alvarez Corona)

"For experimentation, it's great. It's great. However, my question is the opposite. That is, what can be conceived in that space. If you are going to have a marketplace, or an e-commerce, or whatever, where you are going to sell to the entire European territory, this is a direct benefit, without a doubt". (P. Vela)

"Having only one where to compare, surely makes many procedures more agile". (P. Vela)

"This is truly an interesting proposal". (J.M Aguado)

Barriers/Recommendations associated with the initiative

"To apply common sense is to understand the 2080 rules. I mean, for sure, we have plenty of rules that add very little value." (E. Ferro)

"Once we've discovered the areas of weakness in terms of specific services globally, we could look at that data set and find out what the specific services are in different states. Because it's a European project, all the data is open and available on the European Union portal. That's something that could save some effort and provide a good data set for thinking about implementation". (G. Colclough)

"Then, how does it feed into the reality of nation states? It can become something that can't really be applied to any country. Because it can be applied to all of them". (E. Alvarez Corona)

"I think what it should do is lay the groundwork for a minimal pilot that can also be executed in real life, physically. And also tested (...) I recommend the medical field as one testing ground since it merges data, the physical dimension (thus the need of a VW) and regulatory complexity". (E. Alvarez Corona)

"I don't know how this is going to be legislated, but of course we should have all the same taxes." (P. Vela)

"We could actually... Sort of moderators, so to speak. You could conceive a virtual world where we create, again, this role of trusted flagger, where it's not the competent authorities who are involved directly, but we work through an indirect mechanism where we have a first layer of trusted flaggers". (R. Roex)

"I would take another approach, definitely... I don't think we will ever compete on an international level if you let only the SMEs benefit from a regulatory sandbox (...) We need to let go of this focus on small and medium size. We need to give our own big companies a fair chance to innovate on a global plane as well. (...) It's to let Europeans compete with the rest of the world... We will never win if we don't let our big ones compete". (R. Roex)

"It is important also to avoid duplicating horizontal regimes (GDPR, DSA/DMA, Product Safety, AVMSD): Keep it narrow and technical (identity/age, data types unique to VWs), and also temporary and evaluable (to avoid creating a parallel universe of law)". (J.M. Aguado)

"a less enthusiastic agree, only as an optional, narrow, trust-tool-centred sandboxing scheme for startups/micro-enterprises, with no dilution of fundamental rights/consumer and labour protections, strict scope and a sunset.

Another strategy might be to tie-in to AI Act Article 57 sandboxes, allowing VW pilots that include AI agents/content moderation to run inside national AI sandboxes but under a shared VW annex (common metrics, DPIA templates, children's safety checklists)". (J.M. Aguado)

"Sandbox passport might be here a useful option: Single application, single set of trial conditions, mutual recognition across NCAs; joint supervision via an EU coordination node (DG CNECT + Board of Digital Regulators)". (J.M. Aguado)

Opportunities and expressions of interest

"I was recently involved in some proposal regarding Web4, and they wanted, let's say, third-party project (...) to test compared to the legal framework and the regulatory framework". (C. Barelle)

"One is the link between the project and the European Business Innovation Districts Association, something new that's being launched ... So you do indeed have a multiplier in the innovation district partnership. That's where I see the synergy, the enormous potential for synergy to be a delivery tool for the concept of Jurisdiction 28". (G. Colclough)

"One idea that comes to mind is that a town or city not far from where I am right now, Dundee, Scotland, has managed, over the last 15 years, to develop into a massive economy around the gaming industry. I imagine there would be a lot of virtual businesses in that town. As an experimental place to connect, I think it's called the European gaming capital". (G. Colclough)

"For testing ideas in a safe environment, this could be a very interesting idea. Weve had several kinds of health data trading. Weve had the kind of sensitive situations, consent management, copyright management services, where you have to test them in, I mean, to be able to test them in real life, sometimes it is dangerous. But there, I mean, for any items exchange, any items, I said previously data, but any items exchange in this virtual world could emerge without any kind of risks". (T. Papaioannou)

"I would say that I'm (again) cautiously in favour—if it's narrowly scoped and optional, with hard guardrails". (J.M. Aguado)

17 K COMPARATIVE TABLE OF REGULATIONS AND STRATEGIES REGARDING IMMERSIVE TECHNOLOGIES IN THE WORLD

Aspect	European Union (EU)	Japan	South Korea	China	United States (US)
Strategic Framing	<i>Web 4.0 and Virtual Worlds Strategy</i> (COM(2023) 442) – human-centric, rights-based, competitiveness & sovereignty.	“Metaverse Principles” under Society 5.0 – democracy, inclusivity, human rights, industrial competitiveness.	Digital New Deal & Virtual Convergence Industry Promotion Act – aiming for top-5 metaverse market by 2026.	Three-Year Action Plan for the Metaverse Industry (2023–2025) – state-led industrialisation, productivity, national competitiveness.	No comprehensive federal strategy. Fragmented sectoral regulation; industry-driven innovation dominates.
Governance Approach	Multistakeholder, anticipatory governance; strong binding rules (GDPR, eIDAS2, DSA, MiCA).	Soft-law governance via study groups and public–private councils; adaptive legal updates.	Hybrid model – metaverse law + self-regulatory association + ethical codes; sandbox-style experimentation.	State-centric regulation under CAC; heavy content controls, centralised planning.	Fragmented oversight; FTC, SEC, CFTC, FinCEN, state regulators. Enforcement reactive, case-by-case.
Identity & Trust	eIDAS2 and European Digital Identity Wallets – interoperable, trusted digital ID.	No unified e-ID; digital identity via private solutions, under study.	Platform standards; fragmented but tied to child safety & secure ID.	Real-name verification mandatory; state ID integrated into online services.	No federal digital ID; reliance on private authentication; some state-level pilots.

Privacy & Data	GDPR – strict, globally influential data protection.	Adapts existing privacy law; guidance for metaverse data.	Privacy embedded in ethical principles; protection of minors central.	PIPL and Data Security Law enforce localisation, surveillance, and Party oversight.	No federal privacy law. CCPA (California) and state acts fill gaps; FTC intervenes against deceptive practices.
Industrial Policy	Focus on digital sovereignty, competitiveness, interoperability, open standards.	Market projected at ¥24 trillion by 2030; strong focus on creator economy and content industries.	₩200bn+ public investment; support for SMEs, training, and city-scale projects (e.g. Metaverse Seoul).	Industry prioritised in manufacturing, health, education ; global standards influence sought.	Market-driven innovation; venture capital-fuelled; GENIUS Act (2025) anchors stablecoin market; Strategic Bitcoin Reserve launched.
Legal Instruments	Binding regulations: GDPR , eIDAS2 , DSA , MICA .	Amendments (e.g. Unfair Competition Prevention Act) extend IP protection to digital goods; soft-law guidelines.	Virtual Convergence Industry Promotion Act – first dedicated metaverse law; ethics code mandatory.	Cybersecurity Law, Data Security Law, PIPL ; crypto banned; standards set by MIIT.	GENIUS Act (2025) regulates stablecoins; SEC & CFTC divided oversight; CLARITY Act under debate; state privacy acts.

Ethics & Human Rights	Anchored in EU values: inclusivity, accessibility, sustainability, human rights.	Principles stress democracy, inclusivity, and creators as stakeholders.	Ethical code: sincerity, autonomy, reciprocity, privacy, inclusiveness, accountability.	Ethics subordinated to state ideology; “positive energy” content; algorithmic control.	Human rights less central; focus on consumer protection & fraud. Corporate dominance raises monopoly concerns.
Economic & Cultural Dimension	Cultural diversity as asset; citizen panel shaped values; emphasis on public services.	Society 5.0 integrates cultural/creative industries; IP law central.	K-culture (K-pop, Zepeto) drives adoption; strong consumer demand.	Consumer apps secondary to industrial utility; cultural content censored.	Innovation led by Big Tech; strong NFT/crypto subculture; patchwork consumer protections.
Global Engagement	Advocates open, interoperable standards ; active in WSIS, IGF, OECD.	Engages globally but domestic councils lead; values aligned with EU.	Active in OECD, ITU, IGF; exports cultural models.	Seeks to shape global standards; risks creating splinternet .	Fragmented stance; lags in global digital governance fora; extraterritorial reach through market dominance.

18 L. INTERVIEW QUESTIONS

Interview questions

1. From your perspective, what are the most pressing trust-related challenges in virtual worlds today (e.g. identity verification, content authenticity, data governance)?
2. How do users and communities within your platforms currently establish or experience trust, and what are the limitations of these mechanisms?
3. Has your company developed or deployed any specific trust tools—such as decentralised identity systems, content provenance solutions, or privacy-enhancing technologies? Could you walk us through their design and purpose?
4. What role do decentralised technologies (e.g. blockchain, zero-knowledge proofs, verifiable credentials) play in your trust architecture, if any?
5. In building trust-enhancing features, how do you navigate the trade-offs between openness, privacy, interoperability and user safety?
6. What technical, regulatory or cultural barriers have you encountered in implementing or scaling trust tools within your virtual environments?
7. How do you evaluate whether your trust tools are working? Are there particular metrics or feedback mechanisms you rely on?
8. How do you see the governance of trust tools evolving—do you favour decentralised models, industry self-regulation, public standards, or multistakeholder oversight?
9. Looking ahead, what kinds of trust tools or infrastructures do you think will be essential for the future development of virtual worlds?
10. What recommendations would you offer to policymakers or standard-setting bodies who wish to support trustworthy and open virtual ecosystems?

Interviewees

Rutger van Zuidam - Indigo Ventures

Cesare Marzo - Namirial

Saurabh Sing - Siemens

Axel Henriksen - PixelPai

Methodology

1 hour conversation with questions as framework. Answers are not attributable and presented in synthesised form.