Analysis of the Impacts of European Union Regulations and Acts on Virtual Worlds

June 2025

Report Prepared and Published Jointly by

Virtual Dimension Center (VDC) and PEREY Research & Consulting

DOI: 10.6084/m9.figshare.29400131

NOTE: This report is not an ETSI document and is not a deliverable of the STF 686 ViWISSO project.

About the authors

Christoph Runde is a senior standardization expert. With more than 25 years of VR industry experience, he is a pioneer in the field of professional systems and applications of virtual reality and augmented reality. After starting his career at Porsche, he joined the Fraunhofer Institute for Manufacturing Engineering and Automation (IPA) in 1999, where he led the institute's activities in VR/AR. Beginning in 2007 he developed the Virtual Dimension Center (VDC) into one of the biggest and most successful cluster initiatives for VR/AR in Europe.

In parallel to his position as director of VDC, Christoph Runde is professor for Virtual Reality at the Heilbronn University. In the European Association for eXtended Reality (EuroXR) he works as Vice President Industry and End Users. Christoph Runde is the author of the largest database on XR and MV related norms, standards, specifications, guidelines, recommendations, working groups and standard development organizations. He is also the co-chair of the Metaverse Standards Forum's Standards Register WG.

The Virtual Dimension Center (VDC) is Germany's leading competence network for Virtual Engineering. Technology and service providers, users, research institutions and multipliers work together in the VDC network along the entire value chain of Virtual Engineering- namely in 3D simulation, 3D visualization, product lifecycle management (PLM), and Virtual Reality (VR). The VDC maintains a liaison with ISO-IEC JTC1/SC24 Computer graphics, image processing and environmental data representation, and memberships with the Alliance for OpenUSD, App Defense Alliance, Simulation Interoperability Standards Organization (SISO), IEEE Standards, and the Khronos Group.

Christine Perey is a Spime Wrangler. She leads and joins teams working collaboratively to advance business prospects in new technology markets where space and time intersect. Bruce Sterling first used the neologism "Spime" in August 2004 at SIGGRAPH that year. He predicted then that at the intersection of space and time, Spimes would arise. Sterling said "true Spimes create spime wranglers. Wranglers are the class of people willing to hassle with Spimes. And it is a hassle. An enormous hassle. But it's a fruitful hassle. It is the work of progress. Handled correctly, it can undo the harm of the past and enhance what is to come."

PEREY Research and Consulting provides industry-specific knowledge and services packaged the way businesses in fast-moving markets need them—concise, concrete and actionable. Companies leverage the value they receive from working with us in business plans and formulating a variety of mission-critical decisions. We offer agencies of all types, investors, service providers and technology vendors who want to expand their mobile augmented reality communications and community opportunities the tools and the professional partnerships that they need.

Contents

1 Introduction

This report provides information and insights about the relevance and current or potential future impacts on the virtual world technology development and adoption of 11 regulations enacted for enforcement across the European Union. Table 1 lists the full name of the regulations described in this report, their abbreviation, date when enforcement of the regulation or act begins and the date that it went in or goes into full enforcement.

Table 1: EU Regulations Examined in this report

Regulation	Abbreviation	Enforcement Begins	Full Enforcement
Artificial Intelligence Act	AI Act	August 2024	August 2026
Cyber Resilience Act	CRA	December 10 2024	
Data Governance Act	DGA	June 2022	September 2023
Digital Fairness Act	DFA	TBD	TBD
Digital Markets Act	DMA	November 2022	March 2024
electronic IDentification, Authentication and trust Services original and 2.0	eIDAS	Original: 2014 2.0 Core provisions May 2024	Original September 2018 2.0 projected in 2026
European Data Act	ED Act	January 2024	September 2025
General Data Protection	GDPR	May 2018	May 2018
Infrastructure for Spatial Information in the European Community Directive	INSPIRE	May 2007	2021
Interoperable Europe Act	IEA	July 2023	2025
Net Neutrality	None	November 2015	April 2016

The order of examinations of these regulations in this report is alphabetical.

In each chapter, there is first a description of the regulation and its potential significance and impacts on virtual worlds development or adoption. There are also sections about concerns that have been raised by various virtual world stakeholders regarding each European regulation's scope or implementation, and recommendations for possible adjustment or improvements to mitigate negative impacts or reduce barriers.

2 Artificial Intelligence Act

2.1 Overview

The European Union's Artificial Intelligence Act (AI Act) is a legislative initiative aimed at regulating AI systems through a risk-based framework. It categorizes AI applications into four levels: prohibited systems, high-risk systems, low-risk systems, and minimal-risk systems. Prohibited systems include manipulative or socially scoring AI, while high-risk systems used in critical sectors must meet strict requirements for transparency, accuracy, and safety. Low- and minimal-risk systems, such as chatbots or spam filters, face lighter regulations but must maintain transparency. The AI Act also sets standards for data quality, cybersecurity, and human oversight to ensure ethical and safe AI deployment.

The regulation plays a global pioneering role, promoting trust and legal certainty in AI innovation. It emphasizes the protection of fundamental rights of citizens such as privacy and non-discrimination, supporting the responsible and sustainable development of AI. The AI Act not only guides companies but also contributes to international regulatory alignment, potentially influencing global markets by encouraging similar frameworks in other regions.

In virtual worlds, the AI Act has wide-reaching implications. AI systems power user interactions, content generation, and behavioural analysis in virtual environments. The Act requires transparency in how algorithms function, preventing manipulative practices and enforcing fairness. It strengthens data protection by ensuring responsible processing of sensitive personal data such as biometric information and movement profiles. AI-driven moderation must comply with fairness and freedom of expression standards, making virtual spaces safer.

High-risk AI applications in healthcare or finance within virtual worlds would be subject to stricter obligations, promoting user safety and clear accountability. At the same time, the Act allows flexibility for low-risk use cases, facilitating innovation and market entry for smaller providers. Finally, the AI Act encourages interoperability and harmonization across jurisdictions, supporting a consistent, ethical, and competitive framework for AI in the global landscape.

2.2 Concerns

The Artificial Intelligence Act has elicited criticisms concerning its applicability to the virtual worlds from four virtual world stakeholder groups.

Major technology companies, including Google and Meta, have expressed apprehension that the AI Act’s stringent regulations may stifle innovation and place European firms at a competitive disadvantage globally. They argue that the Act’s comprehensive compliance requirements could increase operational costs and delay product launches, potentially hindering the rapid evolution characteristic of AI technologies. Specifically, Meta has encountered delays in deploying AI features for products like the Ray-Ban Meta glasses due to the need to comply with the AI Act’s complex regulatory framework.

In contrast, human rights organizations such as Amnesty International have criticized the AI Act for not going far enough in certain areas. They highlight the Act’s failure to fully ban real-time facial recognition technologies, expressing concerns over potential infringements on human rights and civil liberties. This perspective underscores a perceived regulatory gap that could be exploited within virtual world platforms, where personal data and biometric information are often used and could be exposed.

Some legal scholars have pointed out that the AI Act lacks a comprehensive risk-benefit analysis and relies on broad definitions of AI, which could lead to overregulation. This broad approach may inadvertently encompass deterministic software under the same stringent requirements as more unpredictable machine learning systems, potentially impeding the development of low-risk AI applications within virtual worlds.

In Europe, there is a delicate balance between fostering innovation and ensuring robust regulation. Critics argue that the AI Act’s rigorous compliance obligations could deter startups and smaller enterprises from entering the AI market, consolidating the dominance of established global technology companies. This concern is particularly pertinent to virtual worlds where innovation is driven by a diverse range of actors.

2.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

A more nuanced risk assessment framework than is currently proposed should be implemented to differentiate between various AI use cases within virtual worlds. This is crucial to ensure that low-risk innovations are not subjected to disproportionate regulatory burdens, thereby fostering an environment where novel virtual world applications can flourish without undue constraint. Specifically, tailoring the risk classification to the actual potential for harm in a virtual context will allow for targeted regulation that doesn't inadvertently stifle harmless or beneficial advancements.

Furthermore, fostering ongoing dialogue and stakeholder engagement with industry leaders, civil society organizations, and academic experts is essential. This continuous conversation will ensure the AI Act remains adaptable to the rapid technological advancements inherent in virtual worlds and responsive to the unique challenges they present. Regular forums, workshops, and consultation periods can facilitate this exchange, allowing regulators to gain insights from those directly involved in developing and using these technologies, ensuring the Act's relevance and efficacy over time.

Clarity and precision in the definitions and scope within the AI Act must be increased to prevent overreach and ensure that regulations are precisely targeted. The process of meticulous refinement of the act's text will avoid unintended constraints on innovation by clearly delineating what constitutes an AI system within a virtual world, what specific activities are regulated, and how compliance is to be achieved. Ambiguity can lead to risk aversion and slow down development.

Additionally, introducing measures that support small and medium-sized enterprises in achieving compliance is vital. This includes providing clear, accessible guidelines and practical resources, such as compliance toolkits or simplified reporting mechanisms. Without such support, the burden of compliance could disproportionately affect smaller innovators, leading to a less diverse and potentially less innovative virtual world landscape. This targeted support aims to level the playing field, allowing smaller entities to compete and contribute without being overwhelmed by regulatory complexities.

Finally, proactive monitoring and evaluation of the AI Act's implementation specifically within virtual world contexts should be established. Continuous assessment of implementation practices will help identify unforeseen challenges, measure the effectiveness of mitigation strategies, and inform necessary adjustments to the regulatory framework. This adaptive approach, combined with the other recommendations, will allow the AI Act to better align with the requirements of virtual worlds, fostering an environment that balances innovation with protection of fundamental rights and also promotes a competitive and ethically sound global virtual world ecosystem.

3 Cyber Resilience Act

3.1 Overview

The Cyber Resilience Act (CRA) is a legislative initiative of the European Union aimed at increasing the cybersecurity of digital products and connected services throughout their entire lifecycle. It introduces binding requirements for hardware and software to ensure that products placed on the EU market are designed with resilience against cyber threats. The CRA is part of the broader European cybersecurity strategy and seeks to address growing concerns about vulnerabilities in digital infrastructures, especially in increasingly complex ecosystems such as the Internet of Things and virtual worlds.

The main features of the CRA include the obligation for manufacturers to ensure that products with digital elements meet essential cybersecurity requirements before they are marketed. These include secure-by-design principles, regular updates to address known vulnerabilities, and transparent security documentation. The CRA defines critical product categories with stricter obligations and requires manufacturers to perform conformity assessments and risk analyses. In addition, it introduces a notification duty for security incidents and provides market surveillance authorities with enforcement powers.

In general, the CRA represents a paradigm shift by making cybersecurity a legal obligation rather than a voluntary standard. It increases accountability for developers and suppliers, strengthens trust in digital markets, and aims to reduce the economic impact of cyberattacks. The CRA supports the EU's digital sovereignty and harmonizes cybersecurity rules across Member States. It also promotes a level playing field by requiring all actors—whether inside or outside the EU—to comply with the same standards when offering products in the EU market.

The impact of the CRA on virtual worlds is significant. The development and adoption of virtual worlds depends on complex interactions between devices, applications, and services, all of which are vulnerable to cyber threats. The CRA ensures that display devices, smart contracts, avatars, and decentralized infrastructures meet defined security standards to prevent data breaches, identity theft, and manipulation through insecure software. Ultimately, it contributes to building user trust and operational stability in virtual worlds and immersive environments.

3.2 Concerns

The CRA has prompted concerns from stakeholders regarding its applicability to virtual worlds, encompassing sectors such as social platforms, immersive experience display devices, gaming and digital assets.

The Eclipse Foundation and the Open Source Initiative have expressed that the CRA's broad scope could inadvertently encompass open-source software, potentially deterring volunteer contributions due to liability fears. There is also apprehension that the CRA's stringent requirements may impose significant compliance burdens on companies developing virtual world technologies, potentially stifling innovation and delaying product releases.

Privacy advocates have raised concerns about the CRA's provisions on vulnerability disclosure, suggesting that mandatory reporting of unpatched vulnerabilities could expose systems to exploitation before fixes are implemented. Finally, the decentralized nature of virtual worlds, particularly with blockchain-based platforms and DAOs, presents challenges in assigning liability and ensuring compliance with the CRA, given the absence of a central governing entity.

3.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

The scope and definitions of the CRA need to be clarified with respect to virtual world technologies. The outcome of such a process would clearly delineate its applicability to open-source projects and decentralized platforms, which would prevent unintended liabilities from hindering innovation and collaboration. Without precise definitions, volunteer contributions to open-source software, crucial for the development of virtual worlds, could diminish due to fears of legal repercussions.

Adopting a risk-based approach is essential. This involves implementing tiered compliance obligations based on the specific risk profile of a digital product or service within virtual worlds. Such an approach would ensure that low-risk innovations are not unduly burdened with the same stringent requirements as high-risk components, thereby fostering a more agile and innovative development environment for less critical applications in virtual worlds.

Engaging with stakeholders is also essential. Fostering ongoing dialogue with industry leaders, open-source communities, and legal experts will ensure the CRA remains adaptable to the rapid technological advancements in virtual worlds. This continuous engagement can help identify emerging challenges and opportunities, allowing the regulation to evolve alongside the technology it governs and maintain its relevance and effectiveness.

Finally, specific frameworks must be developed to address decentralization challenges. This involves creating mechanisms that account for the unique structures of decentralized platforms, such as blockchain-based systems and decentralized autonomous organizations. These frameworks should ensure that compliance mechanisms are practical and enforceable within the inherently distributed nature of virtual worlds, preventing regulatory gaps and promoting accountability without stifling the innovative potential of decentralized technologies.

4 Data Governance Act

4.1 Overview

The Data Governance Act (DGA) is a legislative measure of the European Union designed to facilitate the safe and trustworthy sharing of data across sectors and Member States. It aims to establish a governance framework that encourages the re-use of public sector data, supports data altruism, and enables the emergence of secure data intermediaries. The DGA complements other EU data strategies, such as the European Data Act, by providing the institutional and technical foundations for a functioning internal data market.

The main features of the DGA include the regulation of data intermediation services, which must remain neutral and cannot exploit the data for their own purposes. It introduces a certification framework for recognized data altruism organizations and establishes mechanisms to facilitate access to certain categories of protected public sector data,

such as those subject to commercial or statistical confidentiality. The DGA also creates the European Data Innovation Board to ensure coherence in practices and foster interoperability between national data systems.

In general, the DGA is essential for enabling a more competitive and innovation-friendly European data economy. It builds trust among stakeholders by introducing strict requirements for neutrality, transparency, and data security. By enabling voluntary data sharing across industries and borders, it lowers barriers to access while protecting individual and corporate rights. The DGA promotes the development of sector-specific data spaces and supports the broader goal of digital sovereignty within the EU.

The impact of the DGA on virtual worlds lies in its potential to structure data flows and interactions in immersive experiences. Platforms operating in and providing value from virtual worlds must comply with neutrality principles when acting as intermediaries. The DGA facilitates the safe sharing of behavioural, biometric, or usage data between avatars, devices, and services. It supports the creation of interoperable, trust-based virtual world ecosystems and helps prevent monopolization of user data by dominant platforms, enhancing fairness and innovation.

4.2 Concerns

The DGA has prompted concerns from stakeholders regarding its applicability to virtual worlds, encompassing sectors such as social platforms, immersive experience display devices, gaming and digital assets.

European technology firms warn that a cascade of new regulations (including the DGA) could overregulate the nascent virtual worlds ecosystem, burdening innovators and deterring investment. They note that Europe's XR startups already lag behind their U.S. peers in funding, and heavy data-sharing mandates without clear ROI may stall growth. The DGA's one-size-fits-all approach leaves virtual world-specific data (e.g. avatar biometrics or virtual assets) in a gray zone, potentially causing legal uncertainties.

On the other hand, U.S. companies have expressed concern that the DGA's strict data sovereignty rules – such as new limits on transferring non-personal data abroad – could fragment global virtual worlds. Asian governments (e.g. South Korea, Japan) are pursuing pro-innovation virtual world strategies, and observers suggest that overly prescriptive EU rules might put Europe at a competitive disadvantage if they impede cross-border interoperability.

European digital rights groups applaud the DGA's trust-based ethos but flag gaps in privacy protection. They worry that inconsistencies between DGA and GDPR definitions create de facto "double standards," risking weaker safeguards for personal data in immersive environments. There is also concern that DGA's data altruism schemes could expose sensitive user data if not carefully implemented, since highly granular data captured or shared in virtual worlds (health, education, etc.) may be hard to truly anonymize.

Finally, some analysts note that current EU regulations only partially cover virtual world needs – existing laws may not be sufficiently specific about core aspects of virtual worlds like AR display hardware, immersive content and decentralized services. They caution that DGA's model of trusted intermediaries may not fit decentralized, real-time virtual world architectures, posing technical barriers. For example, in trials using virtual worlds for healthcare use cases, data remains "paywalled" and siloed despite DGA's aims, unless deeper cultural changes in data sharing occur.

4.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

Stakeholders across Europe are calling for stronger governance and clarity tailored to virtual worlds. This includes explicitly defining how DGA roles, such as data intermediaries, apply to virtual platforms and avatars, and clarifying interactions between the DGA and GDPR to avoid compliance confusion. Some suggest implementing sector-specific guidelines or regulatory sandboxes to safely trial virtual world data-sharing without stifling innovation.

To prevent the emergence of "walled gardens," experts urge the EC to prioritize interoperability in data governance. They recommend extending DGA and Data Act interoperability requirements to virtual world data formats and identities, ensuring decentralized platforms can exchange data smoothly. Global analysts echo the need for a balance

between frictionless data flows and user privacy, suggesting approaches similar to the EC's Digital Markets Act as a guide for interoperable virtual world ecosystems.

Many advocates urge the simplification and amplification of the DGA's data altruism provisions for virtual worlds. Proposals include streamlining the approval process for data altruism organizations and supporting "data trusts" or commons, where users, companies, and public bodies can voluntarily pool data for mutual benefit. This approach could significantly help sectors like health or education share anonymized immersive data for research and public good.

5 Digital Fairness Act / EU Fitness Check in Digital Fairness

5.1 Overview

The EU Fitness Check on Digital Fairness is a review mechanism assessing whether existing European consumer and competition laws remain effective in a rapidly digitizing economy. It evaluates key directives such as the Unfair Commercial Practices Directive, the Consumer Rights Directive, and the Price Indication Directive, focusing on their suitability in digital contexts. The initiative targets transparency in digital business models, curbing manipulative practices, combating discrimination, and promoting equal market opportunities, particularly for SMEs. It includes broad stakeholder consultations to understand evolving challenges and ensure balanced regulation.

In general, the Fitness Check plays a crucial role in maintaining fairness and competitiveness within the digital single market. As technologies such as AI, big data, and personalized services reshape consumer experiences, the legal framework must adapt. The initiative strengthens consumer rights by enabling informed decisions and shielding users from exploitative tactics. It also fosters a fair competitive environment, discouraging market dominance through unfair practices. Internationally, the EU's leadership in regulating digital fairness influences other jurisdictions and contributes to the harmonization of global standards.

In virtual worlds, where users engage through immersive VR and AR experiences, the Fitness Check becomes increasingly relevant. It ensures transparency in virtual business models by mandating clarity in pricing, terms, and product functionality. This is vital in a space where digital goods and services are often complex. It addresses manipulative strategies like immersive advertising or dark patterns that limit user autonomy. It also ensures algorithms used in content moderation or personalization do not lead to discrimination, maintaining fairness for all users. The Check promotes competition by preventing dominant platforms from marginalizing smaller entrants, thus supporting innovation. Lastly, it enhances consumer trust by reinforcing legal protections and ensuring ethical behaviour from virtual service providers, which is essential for the widespread adoption and legitimacy of virtual worlds.

5.2 Concerns

Stakeholders express contrasting concerns about the EU's Digital Fairness initiative as applied to virtual worlds. Industry groups fear overregulation, warning that layering a new Digital Fairness Act on top of existing laws like the Digital Services Act (DSA) and Digital Markets Act (DMA) could create overlapping mandates. This duplication might stifle innovation and increase compliance costs for businesses operating in virtual environments. These companies urge caution against overly strict interpretations of fairness, which they believe could inadvertently ban legitimate design practices or impose undue burdens on specific platforms.

In contrast, consumer advocates and civil society organizations argue that current consumer protection laws leave significant regulatory gaps in virtual worlds. They point out that existing rules concerning advertising transparency and unfair terms were not designed for the unique characteristics of virtual reality or real-time digital interactions. This creates potential loopholes and practical shortcomings in enforcement, leaving users vulnerable in immersive settings.

Regulators acknowledge issues such as legal uncertainty and fragmentation. They note that the broad principles of the Digital Fairness initiative are challenging to apply to novel virtual world scenarios. Furthermore, inconsistent national approaches risk undermining consumer trust across online platforms.

Academics highlight both the heavy regulatory load already present in Europe and the unmet challenges posed by virtual worlds. These challenges include blurred lines between content and advertising, and complex multi-party liability scenarios. Consequently, they advocate for a balanced yet adaptive approach to regulation.

5.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

To bridge the divides described above, experts suggest tailoring the Digital Fairness initiative to virtual worlds as they evolve over time. Key recommendations include promoting technical interoperability to prevent the creation of walled gardens and ensure healthy competition within the virtual world ecosystem. It is also advised to craft clear standards for immersive advertising disclosures, ensuring users are fully aware when interacting with promotional content in virtual environments. Furthermore, adapting consumer rights for real-time digital interactions is crucial, ensuring users are protected even during instantaneous virtual transactions.

A proactive “fairness by design” mandate could require virtual world platforms to build consumer protections, including transparency mechanisms and privacy safeguards, directly into their offerings from the outset. Regulators are seeking to avoid overreach by coordinating any new rules with existing digital laws and providing clear guidance to industry stakeholders.

6 European Data Act

6.1 Overview

The European Data Act (EDA) is a central regulatory initiative of the EU that aims to promote fair access to and use of data in the digital economy. It focuses on ensuring that data generated through products and services is available to users and businesses, thus enabling innovation and fair competition. Key features include access rights for users and companies to their own usage data, rules for mandatory and voluntary data sharing between companies, strong safeguards to ensure compliance with the GDPR, specific protections for small and medium-sized enterprises, and the promotion of interoperability through widely adopted technical standards.

The EDA plays a vital role in democratizing data access within the EU. It prevents large companies from maintaining exclusive control over valuable datasets, thereby enhancing innovation opportunities, especially in sectors like AI and digital services. It also creates a transparent and fair data economy by strengthening consumer and business rights and by reducing dependencies on dominant platforms through standardized interoperability. The EDA has the potential to serve as a global model for fair data practices and sustainable digital growth.

In the context of virtual worlds, the EDA impacts how data is managed and shared across this immersive, data-rich environment. It ensures that users and developers have access to data generated by their interactions, transactions, or digital creations. This enables them to use the data for further applications, contributing to user empowerment. The act also encourages interoperability between virtual world platforms, allowing users to transfer digital assets and identities more easily. It also prevents data monopolies by requiring dominant platforms to share access with smaller competitors, fostering diversity and innovation. Data protection remains central, especially for sensitive personal data, which must be handled securely and in line with the GDPR. Overall, the EDA supports a fairer and more open virtual world technologies and offerings while strengthening user rights and business opportunities.

6.2 Concerns

Technology companies such as Siemens and SAP have criticized the European Data Act for overregulation and broad data sharing requirements on their companies and those of their customers. They argue that mandatory access to usage and device data may reveal trade secrets and critical intellectual property, potentially weakening Europe’s

global competitiveness. Large platforms also warn that the Data Act, alongside other regulations like the DSA, DMA, and AI Act, creates a regulatory jungle, resulting in high compliance costs, legal uncertainty, and innovation barriers, particularly in immersive environments. They recommend a more flexible framework with voluntary data sharing models and clearer safeguards for proprietary information.

Virtual world start-ups broadly welcome the intention to democratize data access and reduce monopolistic structures. However, they raise concerns about disproportionate burdens and complex compliance requirements that favor larger players. Small firms often lack legal resources to navigate vague definitions and scope.

The European Data Protection Supervisor (EDPS) has warned about insufficient definitions regarding public authority access to data.

6.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

Recommendations for mitigating the concerns raised by stakeholders include simplifying the legal language and providing clear definitions for various types of data within the context of virtual worlds. This simplification is crucial for reducing legal uncertainty and ensuring that both established companies and nascent virtual world startups can experiment with new services under clear legal certainty, without fear of unknowingly violating complex regulations. Furthermore, obligations should be scalable, meaning they are proportionate to the size and resources of the entity, ensuring that smaller firms are not disproportionately burdened by compliance requirements that are more suited for larger organizations.

Industry associations specifically encourage development of stricter safeguards to prevent unfair competitive practices that could arise through data misuse. This involves implementing mechanisms to protect trade secrets and intellectual property when mandatory data sharing is required, thus ensuring that legitimate proprietary information is not exposed to competitors. Additionally, they propose differentiating between business-to-business (B2B) and business-to-consumer (B2C) data sharing scenarios, allowing for more flexible contractual arrangements in B2B contexts. They also advocate for limiting public sector access to data to genuine emergencies, ensuring that governmental data requests are justified and narrowly tailored.

Data protection boards recommend stronger user consent mechanisms tailored for immersive environments and virtual worlds, ensuring that individuals have granular control over their personal data. This includes aligning the EDA's provisions more closely with the GDPR to ensure comprehensive privacy protection for sensitive information, such as biometric data or movement patterns captured in virtual spaces. They also emphasize the need for clear enforcement responsibilities among regulatory bodies and for legal clarity regarding novel virtual world business models, such as those involving NFTs or decentralized platforms.

7 Digital Markets Act

7.1 Overview

The Digital Markets Act (DMA) is a central regulatory tool of the European Union designed to curb the dominance of powerful digital platforms and establish fair competition in digital markets. It targets so-called gatekeepers—large companies with a significant presence across multiple EU member states and wide-reaching digital ecosystems. These include search engines, app stores, social networks, and cloud platforms. The DMA introduces binding obligations such as interoperability, data access, transparency in business terms, a ban on self-favoritization, and greater user autonomy, including the right to uninstall pre-installed software. Enforcement lies with the European Commission, which may impose severe penalties for violations, including fines of up to 10% of global annual turnover.

The DMA’s broader importance lies in rebalancing digital power structures. It empowers small and medium-sized enterprises through fair data access and enables consumers to make autonomous choices in digital ecosystems. It also sets a precedent for global digital governance, potentially inspiring international legislative convergence, which would simplify compliance for globally active companies and promote consistent rules across regions.

In the context of virtual worlds, the DMA has transformative potential. It addresses interoperability, one of the major challenges in this fragmented space, by requiring platforms to allow seamless movement of avatars, assets, and currencies. This could dismantle walled gardens and allow smaller providers to enter and contribute to the virtual world ecosystem. It also ensures that dominant platforms cannot monopolize access to valuable user data such as biometric or behavioural information, reinforcing user privacy and competitive fairness. The DMA prohibits favouritism of proprietary devices or services, which protects competitors from structural disadvantage. By securing fair access, user rights, and open standards, the DMA fosters innovation, diversifies market participation, and strengthens digital self-determination within the emerging virtual world economy.

European officials hail the DMA as vital for an open, competitive virtual worlds. EU Commissioner Thierry Breton argues that the DMA (with the DSA) equips Europe to prevent new “private monopolies” in virtual worlds and uphold EU values. EU reports likewise call for open standards to make virtual worlds “European” . They see the DMA’s “future-proof” design – including powers to add new core services – as ensuring that Web3/XR gatekeepers “will not escape scrutiny” . By contrast, some U.S. regulators decry the DMA as unfairly targeting American firms. A U.S. FTC official slammed looming DMA fines as a “tax on American companies,” voicing suspicion that the law was written to “get at American companies abroad” . This highlights transatlantic tensions, with U.S. stakeholders warning the EU not to overreach.

8.2 Concerns

Major tech companies warn that DMA obligations could undermine security, innovation, and even delay introduction of new virtual world features they will offer in their core products in Europe. Apple, for instance, fears interoperability mandates may compromise user privacy, reportedly hesitating to launch certain AI-powered services in the EU. Industry-aligned analysts argue the DMA favours “static over dynamic competition,” urging a more “permissionless” approach to spur innovation. Smaller tech players and EU startups praise the DMA for curbing gatekeeper abuses. European firms are urging the EU to strongly enforce the act and penalize non-compliance. In mid-April 2025, the EU hit Meta and Apple with Digital Markets Act fines worth hundreds of millions of euros.

8.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

Experts generally support the DMA’s pro-competition aims within virtual worlds, while simultaneously flagging potential gaps that need addressing. European competition scholars, noting the nascent virtual economies within virtual worlds, acknowledge the inherent risks such as the formation of walled gardens and mergers between two or more large providers that could stifle future competition. Consequently, while endorsing the DMA, they strongly recommend vigilant and timely updates to the Act, ensuring its provisions remain effective against evolving anti-competitive practices in the virtual worlds domain as it evolves. This adaptive regulatory approach is seen as crucial for preventing monopolistic structures from solidifying before the virtual world ecosystem fully matures.

Civil society groups largely welcome the DMA as an essential check on the market power of dominant technology companies, yet they also express criticism regarding its original focus primarily on business users rather than explicitly addressing the needs of mass market consumers. A coalition of digital rights non-governmental organizations and academics has specifically urged the integration of user representatives into the DMA's enforcement mechanisms. This inclusion would provide a more direct channel for consumer concerns to be heard and addressed. Furthermore, these groups advocate for preserving encrypted messaging safeguards within virtual worlds, emphasizing the importance of secure communication. Their overarching recommendation is to maintain the openness of virtual worlds while simultaneously bolstering user rights, privacy protections, and technical standards alongside the DMA’s market rules.

9 Digital Services Act

9.1 Overview

The Digital Services Act (DSA) is a legislative cornerstone of the European Union that enhances platform accountability and user rights in the digital environment. As a complement to the Digital Markets Act, the DSA addresses the handling of online content, algorithmic transparency, consumer protection, and the moderation of digital services. It introduces differentiated obligations for platforms based on their size and systemic relevance, with very large online platforms facing the most stringent rules. Key obligations include mechanisms to detect and remove illegal content, transparency in content ranking and advertising, user rights to contest moderation decisions, and special protection measures for minors.

In general, the DSA reshapes the digital ecosystem by demanding social responsibility from platforms while safeguarding innovation. It responds to rising concerns about misinformation, algorithm-driven polarization, and the abuse of online spaces. Beyond the EU, the DSA sets a precedent that may influence regulatory frameworks globally, offering a model for addressing similar challenges in other jurisdictions.

Within the context of virtual worlds, the DSA is poised to play a central role. As immersive environments blur the lines between physical and digital experiences, the risks of harmful content, opaque systems, and data exploitation grow. The DSA could require immersive and AR platforms to implement real-time moderation systems adapted to dynamic, user-generated virtual content. It would also compel them to disclose how algorithms shape experiences, thereby enhancing user trust. Furthermore, it strengthens digital ownership and data rights, enabling users to control their digital identities and assets, while safeguarding minors from immersive threats. Platforms classified as very large must perform risk assessments and prevent abuse. By encouraging interoperability and fair access, the DSA can foster innovation and diversity, preventing monopolistic dominance and supporting an open, inclusive virtual worlds.

9.2 Concerns

Developers warn that the DSA could lead to overregulation of virtual world services across various domains, encompassing gaming, social platforms, education, healthcare, and enterprise collaboration. European game industry groups specifically cite unclear terminology within the Act and the potential for unnecessary administrative burdens on small studios. Furthermore, platform operators highlight practical problems in enforcing strict DSA compliance, noting that moderating complex avatars or 3D environments is significantly more challenging than policing text-based content. U.S. companies also express apprehension that the extraterritorial reach of EU rules could stifle global or regional innovation in virtual worlds.

User advocates, however, argue that the DSA leaves significant regulatory gaps concerning emerging virtual world risks. They point out that immersive environments enable new forms of abuse, such as virtual assaults or child exploitation, which current laws do not adequately address. These advocates strongly urge regulators to recognize and specifically account for these novel harms. Additionally, some caution that overly strict enforcement of the DSA might inadvertently curb creative expression within virtual communities, potentially stifling the organic development of these digital spaces.

9.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

Many European officials acknowledge that the DSA was primarily drafted with static 2D content in mind and therefore requires further adaptation to effectively include innovative and emerging services for virtual worlds. Authorities must specifically clarify how to apply existing DSA definitions, such as illegal content or location, within dynamic virtual worlds. This necessitates conducting ongoing fitness checks as virtual world technology evolves and gains wider adoption, ensuring the regulatory framework remains relevant and effective.

To address these challenges, specific guidance is needed to clarify and adapt DSA rules to 3D environments. For instance, regulators could issue directives allowing for context-specific reporting mechanisms for harmful content in virtual worlds, rather than relying solely on traditional URL-based reporting which is ill-suited for immersive spaces. Furthermore, it is crucial to address new virtual world risks by utilizing the DSA's flexible provisions or, if necessary, introducing new legislative measures to cover virtual world-specific issues. This includes tackling avatar-based abuse, which involves harmful actions perpetrated through digital representations, and deceptive design practices that can mislead users in immersive settings.

Collaboration with stakeholders is seen as paramount to mitigating risks. Through collaboration stakeholders can develop clear codes of conduct and establish regulatory sandboxes in partnership with industry players and civil society organizations. Such collaborative frameworks can help uphold safety standards and ethical behaviour within virtual worlds without stifling innovation, allowing for controlled experimentation and the development of best practices in a real-world context.

10 electronic IDentification, Authentication and trust Services Regulation

10.1 Overview

The Regulation on electronic identification, authentication and trust services (eIDAS) provides a uniform legal and technical framework within the EU for electronic identities and trust services. Its main features include the legal recognition of electronic signatures and trust services, requirements for secure and interoperable electronic identities (eIDs), and the establishment of standardized trust services such as electronic seals, time stamps, and delivery services. These elements aim to ensure the authenticity, confidentiality, and integrity of digital interactions across borders, with a high level of security and legal certainty.

The eIDAS Regulation significantly contributes to the digital transformation of the EU by enabling secure digital transactions and facilitating cross-border access to services. It simplifies administrative processes, reduces reliance on paper documentation, and enhances efficiency for both public and private actors. For people, it enables easier and more secure interaction with digital services. On a global level, eIDAS has set a precedent for how secure digital identity management and trust services can be implemented and recognized internationally.

In virtual worlds, eIDAS plays a crucial role by providing secure and interoperable digital identities. Users could log into different virtual environments using nationally-verified eIDs, thereby enhancing trust and security. For economic activities in virtual worlds, such as digital purchases or smart contracts, eIDAS enables the use of legally valid electronic signatures and seals. This creates a basis for enforceable digital agreements and transactions. The regulation also strengthens protection against identity theft and fraud, as it enforces strict authentication and security standards. Furthermore, eIDAS promotes interoperability between platforms, potentially allowing users to carry verified identities across different virtual worlds. It could ensure legal certainty for digital interactions and reinforces user autonomy by allowing individuals to manage and control their digital identities.

10.2 Concerns

Companies operating in virtual worlds (including very large platform operators) warn that eIDAS 2.0's requirements may be overly prescriptive. They fear that forcing the large platforms to accept EU Digital Identity Wallets and mandating browser recognition of state-issued certificates are seen as heavy-handed. Industry groups argue that the enforcement of eIDAS 2.0 could stifle innovation and impose compliance costs, especially if applied rigidly across virtual worlds offering finance or education services.

Technology firms, both EU and globally, fear the new rules could undermine internet security. Article 45's proposal to trust all EU member-state certificate authorities is criticized for potentially weakening web security and creating single points of failure. A central certificate repository hack, for instance, could compromise thousands of sites (impacting financial transactions and e-health services). Businesses urge revisions to these provisions to avoid new vulnerabilities and to allow flexibility in implementation.

Civil society and user advocates voice strong privacy concerns. They note that the unique, persistent ID envisioned in eIDAS 2.0 could enable cross-platform tracking and profiling of virtual world users. Activists also warn that making a government-issued ID wallet ubiquitous might erode anonymous or pseudonymous participation in virtual worlds – everyday interactions that once required no legal identity could vanish.

10.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

Privacy experts are calling for privacy-by-design improvements such as using service-specific identifiers instead of one universal, employing selective disclosure and zero-knowledge proofs to verify attributes without revealing identity. They also urge robust oversight and legal safeguards to prevent government or corporate misuse of data, ensuring users retain control over their digital identities.

European regulators echo many privacy critiques. The European Data Protection Supervisor (EDPS) flagged the unique identifier proposal as problematic, noting that similar ID schemes have been deemed unconstitutional on privacy grounds; the EDPS recommends exploring less intrusive ways to ensure unique identification. Regulators stress that eIDAS 2.0 must fully comply with GDPR principles across all virtual world use cases.

Experts point out that the draft framework may not yet address certain specific needs for virtual world users. For example, distinguishing human users from bots or avatars in virtual environments is not explicitly covered, posing a gap in digital identity management for future virtual world public services or education platforms. Similarly, the framework should remain adaptable for IoT and immersive technology integrations.

Policy analysts and some EU member states call for clearer governance structures (such as a European Digital Identity Board) to ensure consistent enforcement across regions. They also emphasize the need for open standards and interoperability so that eIDAS identities work seamlessly across different virtual worlds and sectors. This includes allowing multiple certified wallet providers to foster competition and avoid lock-in.

By incorporating these recommendations, stakeholders argue eIDAS 2.0 can better support finance, healthcare, education, and other virtual world services without undue friction.

11 General Data Protection Regulation

11.1 Overview

The General Data Protection Regulation (GDPR) is a foundational legal framework of the European Union that governs the processing of personal data and ensures strong privacy protections for individuals. Applicable to all companies handling personal data within the EU, regardless of their physical location, the GDPR establishes uniform standards for consent, transparency, and user rights. Core features include requirements for explicit consent before data collection, robust user rights such as access, deletion, and data portability, obligations for privacy by design and default, mandatory data breach reporting within 72 hours, and substantial penalties for non-compliance of up to 20 million euros or 4% of global turnover.

In general, the GDPR has transformed global attitudes toward data privacy. It has raised awareness among consumers and forced companies to prioritize data protection as a legal and ethical obligation. For businesses, compliance offers reputational benefits and long-term trust. The regulation has inspired similar laws worldwide, creating a broader international framework of privacy standards. It supports consumers with clear control mechanisms and legal recourse in the event of violations, making data security a central concern in digital business models.

In the context of virtual worlds, the GDPR is especially significant due to the immersive and data-intensive nature of virtual environments. Massive volumes of personal data—biometric, behavioural, and communication-related—are generated. The GDPR mandates informed consent and transparency for data collection and use. Users must be able to access, modify, and delete their data. Privacy must be embedded in platform architecture from the outset, with protective default settings. The regulation also limits profiling and surveillance, requiring explicit user consent for

tracking behaviours. Cross-border data transfers, common in virtual worlds, must meet EU adequacy standards. Platforms must also ensure special protection for minors by securing parental consent and shielding young users from exploitative practices and harmful content.

11.2 Concerns

Virtual world platforms and immersive experience devices collect highly intimate data (e.g. body motion, gaze, facial expressions, vital signs), enabling deeper profiling and "constant monitoring" of users. EU regulators like the EDPS warn that virtual worlds can even capture special-category data (physiological or emotional cues such as gait, eye movements, or heart rate) revealing sensitive traits. This raises major compliance concerns under GDPR's limits on processing sensitive biometric data. Scholars argue GDPR's traditional "informed consent" model falters in immersive environments.

Users in virtual worlds cannot realistically grasp or control the continuous, subtle data collection (for example, eye-tracking influencing their experience) – making text privacy notices effectively hollow. In short, privacy self-management becomes impractical when AI-driven worlds constantly react to biometric signals.

Legal analysts indicate GDPR is not fully equipped for novel data practices such as those in virtual worlds. For instance, issues like AI-driven avatars, reality capture (e.g. scans of 3D environments), and blockchain-based virtual assets raise questions GDPR doesn't clearly answer. Observers note that applying GDPR to virtual worlds "provides a stress test" for the law, and call for clarifications – even amendments – regarding consent requirements, cross-border data flows, and new data categories.

11.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

European experts propose expanding GDPR's scope – for example, treating emotion, neurodata and other inferred mental-state information from immersive experience and human interface devices as "sensitive data" subject to strict protection. This could mean amending GDPR to add new categories of protected data, ensuring biometric emotion data and cognitive privacy receive the same rigor as health or biometric identifiers. Some even advocate new rules addressing mental integrity to prevent manipulative profiling beyond current GDPR provisions.

Civil society groups and researchers urge moving beyond click-through consent toward built-in privacy protections. Proposed solutions include user-controlled privacy dashboards in VR, real-time indicators or visualizations of what personal data is being captured, local (on-device) processing to minimize data sharing, and automated blurring of bystanders in AR environments. Such privacy-by-design measures would operationalize GDPR principles (like data minimization and transparency) in virtual world interfaces.

U.S. and global industry stakeholders caution against treating virtual worlds with wholly new or overly rigid rules. The Information Technology and Innovation Foundation recommends a technology-neutral approach – focusing on the types of data and actual harms involved – rather than VR- or AR-specific regulations, so as not to stifle innovation.

Similarly, business coalitions such as the OECD, advocate coherent, broadly accepted privacy frameworks that protect users without impeding innovation. Startups and other organizations (like XRSI) emphasize a multi-stakeholder, context-specific strategy: one-size-fits-all compliance is tricky, so guidance should adapt to different virtual world use cases and share best practices proactively across the ecosystem.

12 INSPIRE Directive

12.1 Overview

The INSPIRE Directive (Directive 2007/2/EC) is a European Union legislative act aimed at establishing a European Spatial Data Infrastructure to enable the sharing of environmental spatial information among public sector

organizations and improve environmental policy-making across the EU. Its primary objective is to facilitate the interoperability and harmonization of spatial datasets and services, ensuring that geographical information is easily accessible and usable for cross-border and cross-sectoral applications.

The main features of the INSPIRE Directive include the creation of metadata standards, common specifications for spatial data sets and services, and obligations for public authorities to make data discoverable and accessible through network services such as view, download, and transformation services. It covers 34 spatial data themes, including transport networks, land cover, geology, and human health, structured into annexes. The directive also mandates coordination among EU Member States and promotes transparency and reusability of spatial data.

In general, the INSPIRE Directive plays a foundational role in building a coherent spatial data ecosystem in the EU. It supports better governance by improving access to location-based information and contributes to digital transformation through standardized data interoperability. It enables more effective environmental monitoring, disaster response, and urban planning. The directive also reduces redundancies and enhances collaboration among public and private stakeholders by ensuring that spatial data can be reused efficiently.

The impact of the INSPIRE Directive on virtual worlds lies in its ability to provide standardized and reliable geospatial datasets that can be used in the construction of virtual environments. For virtual worlds platforms incorporating real-world mapping, urban simulation, or digital twins, INSPIRE-compliant data ensures consistency and accuracy. It facilitates cross-platform interoperability and integration of geographic features into immersive applications. By aligning virtual world developments with public data infrastructures, the directive enhances realism, usability, and regulatory compliance in virtual space design.

12.2 Concerns

Some public authorities argue that INSPIRE is too rigid and technologically outdated to serve the needs of the as of yet undefined virtual world. Its emphasis on 2D environmental datasets does not accommodate the dynamic, immersive 3D/4D spatial models central to virtual governance, digital twins, or VR-based urban planning. INSPIRE's strict schema and compliance obligations could impede innovation, particularly in smart city applications involving real-time data and AR overlays.

Private sector stakeholders and developers criticize INSPIRE's legacy infrastructure, which relies on complex XML schemas and outdated service interfaces. These are incompatible with lightweight, modular formats and real-time rendering engines used in AR/VR, immersive and game-based environments. Developers face challenges in integrating INSPIRE-compliant data with glTF, 3D Tiles, or Unity engines. Licensing and reusability restrictions on public spatial data also limit creative and commercial virtual world use cases.

NGOs and civil society groups support the open data spirit but criticize uneven implementation across EU member states. Critical datasets are often missing or incomplete. INSPIRE's regional scope excludes most non-EU countries, which hampers spatial interoperability in cross-border or humanitarian virtual world use cases.

12.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

A framework complementary to INSPIRE could be developed to adopt modular, tech-neutral standards, integrate 3D/4D real-time data natively, and support REST APIs and open licensing.

If undertaken, a new spatial data initiative would need to be co-designed with public and private actors to balance flexibility and interoperability. Global alignment, particularly through UN and ISO efforts, is essential. To address emerging needs, the future spatial data infrastructure framework should also include ethical guidelines, user rights in digital space, and sustainability protocols.

13 Interoperable Europe Act

13.1 Overview

The Interoperable Europe Act is a legislative initiative of the European Union that aims to strengthen cross-border interoperability and cooperation in the public sector across the EU. Its purpose is to facilitate the seamless exchange and reuse of data, services and digital solutions between administrations, businesses and people. The act provides a legal and organizational framework for promoting digital sovereignty, transparency and efficient service delivery through common standards and infrastructures.

The main features of the Interoperable Europe Act include the establishment of a structured governance model for interoperability, the creation of a shared catalogue of reusable digital solutions and components, and the implementation of common interoperability assessments for public sector projects. It also provides for cooperation mechanisms among Member States and the European Commission, supported by the Interoperable Europe Board. Key instruments such as the European Interoperability Framework and interoperability testing environments are anchored in the act to ensure consistency and measurable progress.

The importance of the Interoperable Europe Act lies in its role as a catalyst for administrative modernization and digital resilience in the EU. It reduces administrative burdens, enables better policymaking through improved data flows, and fosters the reuse of digital solutions across borders. By setting legal guarantees for open standards and interoperability-by-design, the act enhances transparency and accountability. It also contributes to the EU's digital decade objectives by ensuring coherent digital public services and better alignment with other digital legislation, such as the Data Governance Act and the Digital Services Act.

In the context of virtual worlds, the Interoperable Europe Act could serve as a blueprint for ensuring that public sector representations and services in virtual environments are compatible and accessible across platforms. It would support the development of open virtual world infrastructures, particularly in areas such as digital identity, e-government portals and virtual citizen services. The act promotes standardization and interoperability principles that are essential for creating inclusive and connected virtual world ecosystems.

13.2 Concerns

The EU's Interoperable Europe Act has drawn criticism when applied to broader contexts for which it was not originally intended. Public bodies note that virtual worlds are borderless and will require international governance beyond any one region's rules. Industry voices caution that a prescriptive EU approach could prove inflexible, and some fear a few dominant platforms could still form closed ecosystems that stifle competition.

Civic organizations stress that interoperability should not trump user rights, urging that cross-platform systems uphold privacy and safety by design. Academic experts argue the Act reflects legacy assumptions, suited to web-era data exchange but ill-equipped for immersive, real-time interactions in virtual worlds. They warn that the EU's current rhetoric of fostering multiple virtual worlds could lead to incompatible silos and new digital divides, exposing gaps in addressing 3D/4D content standards and live interoperability.

13.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

Experts and institutions recommend a dedicated governance layer to complement the Act and tackle interoperability challenges specific to virtual worlds. A top suggestion is to create a global, multi-stakeholder process to coordinate technical standards for virtual worlds, beyond the remit of existing internet or standardization bodies. Flexible regulatory sandboxes are proposed so innovators can pilot immersive services under lighter rules, mitigating the risk that strict regulations hamper experimentation.

To enable seamless digital identity across platforms, the use of decentralized identity frameworks (e.g. EU's eIDAS 2.0 wallets) is encouraged. Stakeholders urge development of open standards for avatars, 3D assets, and real-time data sharing through international standard-setting collaborations.

14 Net Neutrality Regulation

14.1 Overview

The Net Neutrality Regulation ensures that internet service providers treat all data traffic equally, prohibiting discrimination, blocking, throttling, or paid prioritization of content, services, or applications. Introduced by Regulation (EU) 2015/2120, it mandates transparency from providers regarding service quality. This regulation aims to preserve an open and fair internet environment by preventing preferential treatment based on commercial agreements and ensuring uniform access for all users.

Net neutrality is essential to preserving the structural integrity of the internet. It prevents dominant players from gaining unfair advantages and protects small providers and start-ups from exclusion. Consumers benefit by being able to access digital content and services without interference or bias, fostering freedom of expression and diverse media landscapes. Internationally, the principle supports global competitiveness, avoids market concentration, and serves as a benchmark for other jurisdictions considering similar frameworks.

In the context of virtual worlds, which relies on high-bandwidth, low-latency connections for VR and AR experiences, net neutrality plays a critical role. Equal access to all virtual environments ensures that no virtual world platform is disadvantaged or privileged based on ISP partnerships. This promotes diversity and user freedom in choosing content and services. It also encourages innovation by giving start-ups equal opportunities to develop and distribute new applications without being marginalized by data prioritization practices.

The regulation directly supports a consistent and high-quality user experience by ensuring uninterrupted and equitable data flow across all platforms. Without it, ISPs could selectively slow down competitors or prioritize dominant services, degrading inclusivity and functionality of virtual worlds. Furthermore, net neutrality reinforces user rights by protecting against commercial manipulation of access and experience. It sustains a competitive digital ecosystem where creativity, choice, and user autonomy are preserved regardless of corporate influence or financial capacity.

14.2 Concerns

Telecommunication network operators argue that strict net neutrality rules hinder the delivery of latency-sensitive virtual world services. In regions like the EU, legal uncertainty surrounds practices such as 5G network slicing, which are essential for real-time applications like VR, digital twins, or telemedicine. Operators claim that current frameworks disincentivize investment and prevent optimized service delivery.

Developers and platform providers, however, strongly support net neutrality to prevent ISPs from throttling or monetizing access to immersive experiences or services. Civil society groups warn that allowing fast lanes could create a two-tier internet, where startups or public-interest platforms are disadvantaged if they cannot afford prioritization.

Regulators and academics note structural gaps. Traditional neutrality laws, built for static content, are increasingly mismatched with immersive, high-throughput, real-time environments. The European Commission acknowledges that some flexibility may be required for critical services, but fears regulatory rollback.

14.3 Mitigation

This clause describes potential steps for mitigating the impacts expressed by the stakeholders in the clause above.

Experts propose allowing conditional and transparent prioritization for verified latency-sensitive services, such as immersive education, telehealth, or emergency response applications within virtual worlds. This prioritization,

however, must apply equally to all providers offering similar critical services and must be technically justified, with clear criteria, to prevent any anti-competitive behavior or preferential treatment. The aim is to balance the need for optimized performance in real-time immersive experiences with the core principle of an open internet.

Furthermore, regulatory frameworks should enforce strong transparency in traffic management. This means that any prioritization deals made by internet service providers must be fully disclosed and subjected to regular audits by independent bodies. This ensures accountability and helps to identify any discriminatory practices that could undermine net neutrality. Additionally, net neutrality principles should be extended to dominant virtual platforms themselves to prevent them from discriminating against or disadvantaging other services or content within their own virtual environments, thereby ensuring fair access for all participants in the virtual world ecosystem.

Finally, global alignment on these principles is highly recommended. While retaining the core principles of open access and non-discrimination that are core to European values, net neutrality in the virtual world era must adapt to include considerations for real-time performance needs. This includes addressing platform-level fairness and implementing safeguards against monopolistic throttling or exclusionary practices.

15 Conclusion

15.1 Introduction

Regulatory frameworks such as the AI Act, Data Act, eIDAS, Digital Markets Act (DMA), and INSPIRE Directive provide important legal foundations for safety, fairness, and innovation for emerging virtual worlds. These laws enhance trust, protect user rights, and foster open competition. The DMA and Data Act support interoperability by enforcing data access and banning self-preferencing by dominant platforms. The INSPIRE Directive supplies reliable spatial datasets for virtual twin environments, while eIDAS ensures secure digital identities.

Standardisation initiatives embedded in these laws reduce fragmentation, enabling cross-border services and simplifying compliance across sectors. The Cyber Resilience Act raises security standards by embedding secure-by-design principles in XR products and smart contracts. Together, these instruments help build a resilient, interoperable digital infrastructure essential for stable and equitable virtual world ecosystems.

While there are many benefits, there are also concerns. Stakeholders across sectors warn that overregulation could stifle innovation, especially among SMEs and startups. Laws like the AI Act and CRA are seen by industry leaders as too complex and cost-intensive, potentially delaying time-to-market. Critics also argue many frameworks—such as INSPIRE and the Interoperable Europe Act—reflect legacy assumptions that don't address 3D/4D data, real-time processing, or immersive interaction. Civil society stakeholders raise parallel concerns: the GDPR's consent model struggles in immersive contexts where continuous biometric tracking is difficult to regulate meaningfully. Standardisation efforts, while beneficial, are often fragmented across directives, leading to interoperability gaps, legal uncertainty, and inefficiencies in cross-platform immersive experiences.

15.2 Gaps

Several regulatory gaps related to virtual worlds have been identified across existing EU and global frameworks. Many laws are built for static, 2D web environments and fail to address core aspects of immersive, real-time virtual spaces. For example, the INSPIRE Directive lacks support for 3D/4D spatial data and real-time AR applications. The GDPR struggles to manage continuous biometric tracking and inferred emotion data typical in XR platforms. The Cyber Resilience Act does not yet account for decentralized systems like DAOs, leaving enforcement unclear. Similarly, eIDAS 2.0 risks undermining anonymity and user privacy by enforcing uniform digital ID schemes without flexible safeguards. The Interoperable Europe Act is seen as too Eurocentric, lacking global coordination needed for borderless virtual environments. Overall, these gaps reflect outdated assumptions, limited standardisation coverage, and insufficient alignment across data governance, digital identity, and spatial interoperability—raising legal uncertainty and technical friction in virtual world technology development.

15.3 Recommendations with focus on standardisation

Experts call for a complementary governance layer tailored to virtual worlds that aligns legal instruments with dynamic, immersive technologies. Regulations should incorporate flexible, risk-based approaches, distinguishing low-risk innovation from high-risk applications. EU bodies are urged to develop modular, tech-neutral formats like 3D Tiles, REST APIs, and decentralized identity protocols. The INSPIRE Directive should be extended to support real-time geospatial streaming and virtual mapping using modern formats. The Interoperable Europe Act should coordinate with international actors to prevent siloed virtual world platforms and infrastructures.

To address decentralization, laws like the CRA and DGA must clarify liability and compliance responsibilities for DAOs and open-source systems. Sandboxed regulatory environments are recommended to test virtual world applications without stifling experimentation. Privacy regulations like GDPR and eIDAS must embrace privacy-by-design tools such as zero-knowledge proofs, selective disclosure, and local data processing. Finally, virtual world-specific task forces are proposed to develop cross-sector interoperability standards for avatars, digital identities, and spatial data layers. This would ensure that Europe’s regulatory model remains future-proof while fostering a globally interoperable, innovation-friendly virtual world ecosystem.