

D3.2: Regulatory Gap Analysis - Summary

The Regulatory Gap Analysis report by XR4Human examines 25 key European Union (EU) regulations and directives and their applicability to XR technologies and virtual worlds. This summary provides a very brief overview of the regulations identified as relevant and their implications for XR.

Authors: Miltos Ladikas, Octavia Madeira, Julia Hahn (KIT), Marco Correa Pérez, Pascal Musyoki, Dhruv Somayajula (ULEI)

Editors: Miltos Ladikas (KIT), Marco Correa Pérez (ULEI)

Find full version of report here: <https://zenodo.org/records/14045412>

1. Privacy and Data Regulations

- General Data Protection Regulation (GDPR): Governs personal data protection. XR applications must comply with strict consent rules and rights, such as the "right to be forgotten," particularly when collecting biometric data like facial recognition, eye movement and gait patterns.
 - e-Privacy Directive: Protects privacy in electronic communications. XR platforms enabling real-time user interactions (e.g., multiplayer VR) may face compliance demands.
 - Data Act (DA): Focuses on fair access to and sharing of data. XR companies could benefit from accessing broader datasets, enabling enhanced applications and immersive experiences.
 - Data Governance Act (DGA): Establishes frameworks for sharing data altruistically. XR can leverage shared public sector data (e.g. healthcare or mobility) to improve applications while ensuring compliance.
-

2. Intellectual Property

- Directive on Copyright in the Digital Single Market: Provides rules for using copyrighted content in digital spaces. XR platforms must manage user-generated content to avoid unintentional copyright violations.
 - Regulation on EU Trademarks: Protects trademarks in the digital economy. XR marketplaces must safeguard against unauthorized use of trademarks in virtual environments.
 - Directive on the Protection of Trade Secrets: Secures proprietary information. XR developers must ensure robust data protection to safeguard trade secrets in shared virtual worlds.
-

3. Consumer and Competition Law

- Consumer Rights Directive (CRD): Mandates transparency and fairness in consumer contracts. XR providers must ensure user-friendly and clear terms for virtual goods and services.
- Digital Content Directive (DCD): Governs quality and fairness of digital products. XR applications must meet reliability standards and address content defects.
- General Product Safety Regulation: Requires safe product design. XR hardware and software must comply with safety standards to avoid risks to users.

- Unfair Commercial Practices Directive (UCPD): Prohibits deceptive marketing. XR providers must ensure accurate representations of virtual products and services.
-

4. Media and Online Services

- Audiovisual Media Services Directive (AVMSD): Regulates media services, including XR content delivery. XR platforms must address rules on advertising and age-appropriate content.
 - Digital Services Act (DSA): Focuses on platform accountability. XR platforms hosting user-generated content must implement content moderation to combat illegal activities.
 - Digital Markets Act (DMA): Addresses monopolistic behaviors. XR developers must ensure fair competition when participating in XR ecosystems dominated by big-tech companies.
-

5. Cybersecurity

- Network and Information Security Directive (NIS2): Establishes cybersecurity protocols. XR platforms must protect against threats like identity theft or system breaches.
 - Convention on Cybercrime: Provides frameworks for combating cybercrimes. XR providers must collaborate to address cyber-related risks in virtual worlds.
 - Child Sexual Abuse Regulation: Imposes safeguards against exploitation. XR platforms must implement measures to prevent abuse and illegal content distribution.
-

6. Accessibility and Non-Discrimination

- European Accessibility Act (EAA): Requires inclusivity in digital products. XR providers must ensure accessible design for people with disabilities.
 - Web Accessibility Directive: Governs accessibility of online services. XR platforms must ensure interfaces are inclusive for all users.
-

7. Health Law

- Clinical Trials Regulation: Ensures the safety of health-related XR applications. XR technologies used in healthcare must meet rigorous testing and reporting standards.
 - Medical Devices Regulation: Sets rules for medical devices. XR applications in medical diagnostics and treatment must comply with safety and efficacy requirements.
-

8. Technology-Specific Law

- Artificial Intelligence Act (AI Act): Regulates AI applications. XR platforms using AI (e.g., behavioral analytics) could be considered high risk and must address strict ethical and transparency concerns.
-

9. Finance Law

- Anti-Money Laundering Directive (AMLD): Prevents misuse of financial systems. XR marketplaces must implement safeguards against illicit transactions.
 - Electronic Money Directive (EMD): Governs digital payments. Virtual economies in XR must comply with secure and transparent e-money practices.
 - Markets in Crypto-Assets Regulation (MiCAR): Regulates cryptocurrencies. XR platforms dealing with NFTs or virtual currencies must ensure compliance with this regulation.
 - Digital Operational Resilience for the Financial Sector (DORA): Enhances financial system resilience. XR platforms managing financial transactions must address operational risks.
-

Key Takeaways for XR

The regulatory landscape for XR technologies and virtual worlds is extensive and multifaceted. Compliance with these laws requires a robust understanding of privacy, safety, accessibility, intellectual property, and competition laws. The Regulatory Gap Analysis emphasizes the need for harmonized, technology-neutral regulations to foster innovation and ethical development in XR.