XR4 HUMAN

D3.2: Regulatory gap analysis

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

Project title: The Equitable, Inclusive, and Human-Centered XR Project

Project acronym: XR4Human

Grant Agreement no.: 101070155
Lead contractor for this deliverable: KIT

Funded by the European Union

Deliverable factsheet:

Project Number:	101070155
Project Acronym:	XR4Human
Project Title:	The Equitable, Inclusive, and Human-Centered XR Project
Title of Deliverable:	D3.2 – Regulatory gap analysis
Work Package:	WP 3 - Mapping of the Regulatory and Governance Issues of XR
Due date according to contract:	M24
Editor(s):	Miltos Ladikas (KIT), Marco Correa Pérez (ULEI)
Contributor(s):	Miltos Ladikas, Octavia Madeira, Julia Hahn (KIT), Marco Correa Pérez, Pascal Musyoki, Dhruv Somayajula (ULEI)
Reviewer(s):	Alina Kadlubsky (OARC EU)
Approved by	Rigmor C. Baraas (USN)

ABSTRACT:	The report analyses relevant to XR EU legislations (twenty five in total), clustered into privacy and data, intellectually property, consumer and competition law, media and online services, cybersecurity, accessibility and non-discrimination, sectoral law, technology law, and finance law. The gap analysis highlights the scope, subjects, main provisions and applicability of each regulation to the XR sector. The challenges that XR technologies are faced with are discussed in terms of barriers, uncertainties and conflicting requirements in the existing regulatory landscape. The analysis reveals a multi-faceted regulatory framework impacting all entities and all sectors that provide XR products or services to the European market. XR technologies often introduce novel concerns or newer dimensions of existing concerns. The processing of biometric personal data, the potential of identity theft online or the role of data inequality, highlight the importance of technology-neutral laws that can accommodate these newer dimensions of normatively understood concerns. The pace of XR technological developments is overtaking the ability of policy making to offer adequate regulatory coverage of the issues they bring up to the forefront. There is therefore a need to foster adaptable regulations that can be readily

	updated in tandem with the development of XR technologies. The regulatory gap analysis provides the backbone for the forthcoming policy roadmap to ensure a comprehensive and ethical XR technology development.
Keyword List:	Extended Reality, Virtual Reality, Augmented Reality, data protection, intellectual property, consumer law, cybersecurity, health law, finance law, EU law.

Consortium:

	ROLE	NAME	Short Name	Country
1.	Coordinator	UNIVERSITETET I SOROST-NORGE	USN	NO
2.	Partner	XR4EUROPE	XR4Europe	BE
3.	Partner	UNIVERSITETET I OSLO	UiO	NO
4.	Partner	ETHNICON METSOVION POLYTECHNION	NTUA	EL
5.	Partner	NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU	NTNU	NO
6.	Partner	UNIVERSITEIT LEIDEN	ULEI	NL
7.	Partner	KARLSRUHER INSTITUT FUER TECHNOLOGIE	KIT	DE
8.	Partner	INSTITUTT FOR ENERGITEKNIKK	IFE	NO
9.	Partner	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	Fraunhofer	DE
10.	Partner	OPEN AR CLOUD EUROPE GEMEINNUTZIGE UG	OARC EU	DE
11.	Partner	STICHTING FONTYS	Fontys	NL
12.	AP	UNIVERSITY OF LEEDS	UNIVLEEDS	UK

Revision history:

VERSION	DATE	Revised by	Reason
0.1	13 September 2024	-	First draft
0.2	15 October 2024	Alina Kadlubsky	Peer internal review
0.3	27 October 2024	Rigmor C. Baraas	Second draft
1.0	28 October 2024	-	Final version

Table of contents

Funded by the European Union

Funded by the European Union

1. Introduction

The project XR4HUMAN focuses on an ethical and human-centered development process for XR technologies. It involves representing industry, consumers, regulators, and academia to generate European standards for XR. As described in its basic concept, the project supports end-user decision-making and, through a focus on inclusivity, ensures that every European company and citizen has the potential to take advantage of what XR can offer. This will pave the way towards a strong and competitive ecosystem while building public trust and acceptance.

In a previous report, we analysed the use of XR technology in various sectors, including media and entertainment, work and production, marketing, healthcare, security, education, Urban Planning and Conservation.[1] The use of XR technology in these sectors highlights its potential and benefits while also indicating potential risks posed by XR adoption, which may impact individuals unless mitigated appropriately. Keeping these risks in mind, we seek to review the extant regulatory framework in the EU that intersects with the ethical and policy issues raised by XR technology in this report. Considering that XR technologies potentially cover a wide range of applications, the applicable regulations also cover most societal activities. Since, at this stage, it is not prudent to predict the XR applications that will have the strongest impact on society and will therefore require a stricter regulatory timeline, we have opted to cover the widest possible regulatory areas that could be affected by XR developments. We have clustered the regulations into their main focus: privacy and data, intellectually property, consumer and competition law, media and online services, cybersecurity, accessibility and non-discrimination, sectoral law, technology law, and finance law (see below for details).

Topic	**Name**
Privacy and Data	General Data Protection Regulation (GDPR)
	e-Privacy Directive
	Data Act
	Data Governance Act
Intellectual property	Directive on Copyright in the Digital Single Market
	Regulation on the EU Trademarks
	Directive on the Protection of Trade Secrets
Consumer and competition law	General Product Safety Regulation
	Unfair Commercial Practices Directive (UCPD)
	Consumer Rights Directive (CRD) and its Guidance

[1] 'D3.1: State-of-art in XR Policy Debates', The Equitable, Inclusive, and Human-Centered XR Project (2023)

	Digital Content Directive (DCD)
Media and online services	Audiovisual Media Services Directive (AVMSD)
	Digital Services Act (DSA)
	Digital Market Act (DMA)
Cybersecurity	Network and Information Security Directive (NIS2)
	Convention on Cybercrime
	Child and Sexual Abuse Regulation
Accesibility and Non-Discrimination	European Accesibility Act (EAA)
	Web Accessibility Directive
Health law	Clinical Trials Regulation
	Medical Devices Regulation
Technology law	Artificial Intelligence Act (AI Act)
Finance law	Regulation for the Digital Operational Resilience for the Financial Sector (DORA)
	Anti-Money Laundering Directive (AMLD)
	Electronic Money Directive (EMD)
	Markets in Crypto-Assets Regulation (MiCAR)

The report is divided into a section per regulation, and it is structured to highlight the salient features of the law (scope, subjects, main provisions), followed by a discussion on its applicability to the XR sector. The analysis provides an overview of the challenges that XR are faced with in terms of their applicability in relation to the specific law, identifying potential gaps that must be dealt with to allow for a smooth adaptation to XR or even instances of over-regulation whereby conflicting requirements pose barriers for the applications of XR technologies. This part of the study will form the backbone for the next stage in the project analysis, which aims to develop a policy roadmap for XR technologies.

2. Glossary

- AR: Augmented reality
- CJEU: Court of Justice of the European Union
- CoE: Council of Europe
- EC or Commission: European Commission
- EEA: European Economic Area
- EU: European Union
- EU Official Journal: Official Journal of the European Union
- MR: Mixed reality
- MS: Member States (of the European Union)
- N-IICS: Number-Independent Interpersonal Communication Services
- VR: Virtual reality
- XR: Extended reality

3. Privacy and data

3.1. General Data Protection Regulation

1. Overview of the regulation

1.1. Scope

The Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (known as **General Data Protection Regulation** or **GDPR**), was published on 27 April 2016[2].

GDPR is the main EU personal data privacy law that has been in effect since 25 May 2018. It has been incorporated into national legislation throughout MS, and it is designed to give individuals more control over how their data is collected, processed, and protected online. To achieve maximum effects, GDPR binds organisations to strict rules on accumulating and processing personal data they collect from people. It provides details on the mandatory use of technical safeguards, e.g. encryption, and requires a demanding level of justification for personal data collection. It is the most comprehensive legislation of its kind at the global level and levies heavy penalties on organisations that break its requirements: up to 4 per cent of the organisations' global annual revenue or €20 million, whichever is higher.

1.2. Subjects

GDPR recognises as 'data subjects' any individual whose personal data has been recorded, processed or accumulated for any purpose. As such, the definition of personal data in the regulation is vital in order to understand its functions[3]:

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

It then clears that GDPR provides a wide view of personal data and allows for the possibility of individual identification through a combination of otherwise anonymised/pseudonymised data. For instance, the combination of anonymous location data, internet protocol address, cookie identifiers and online postings might be able to identify a person, and therefore such data are liable under GDPR provisions. Moreover, the nature of data that can be processed can be anything from name, address, skin colour, opinions, etc. In contrast, data processing includes all possibilities, such as gathering, storing, transmitting, analysing, etc. At the same time, GDPR covers data processed outside the EU, even from entities without connection with the EU, as long as they involve EU citizens' data.

In effect, the outreach of GDPR is immense across the globe and relates by default to the activities of most international companies. The most severe (and most publicised) penalties resulting from breaching GDPR obligations have been given to conglomerates such as Meta, Google, Amazon and TikTok[4]. So far,

---

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[3] Article 4, GDPR

[4] https://www.eqs.com/compliance-blog/biggest-gdpr-fines/

almost all investigations and fines focus on businesses processing personal data and very rarely on public institutions or individuals.

1.3. Main provisions

(a) Principles

GDPR states seven key principles on data processing that must be followed in order to avoid penalties for non-compliance[5]:

- Processing must be lawful, fair and transparent to the EU citizens as data subjects.
- Data can only be processed for legitimate reasons clearly spelt out to the data subject.
- Data minimisation must be in practice.
- Data accuracy and timeliness must be adhered to.
- Storage limitation and purpose limitation on information in that it can only be kept for the least possible time.
- All processing of data and data flows must ensure security, confidentiality, and integrity.
- The data controller is accountable for compliance with GDPR protection privacy laws.

These general principles permeate the whole regulation and provide the structure for its content. Overall, the main provisions of GDPR are evolving around the lawfulness of data processing, the rights of the data subjects, and data governance (controller and processor).

(b) Lawfulness

Article 6 sets the tone for the lawfulness of data processing by describing in which case data processing is lawful. One of the following must apply[6]:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child.

Individual consent is the most straightforward manner to establish lawfulness in data processing. The other cases assume contractual interactions or are based on public interest, in cases other relevant regulations overlap [7]. However, we must assume that most XR applications will base the lawfulness of personal data processing on individual consent, regardless of the nature of their contractual obligations. This is the case with any main commercial activity based on personal data processing.

[5] Article 5, GDPR
[6] Article 6, GDPR
[7] See Digital Services Act and Digital Markets Act sections

(c) Rights of subjects

Article 15 describes one of the key rights of individuals in the GDPR, that is, the right to know what personal data is accumulated and processed. The specific rights are[8]:

(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Moreover, where personal data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer. The controller shall provide a copy of the personal data undergoing processing[9]

As one can easily deduce from the above that GDPR gives individuals significant powers in relation to their personal data. Not only do people have the right to access their data in any case and from any entity that holds it, but they can also request extensive information about their data's use and processing possibilities. Moreover, any individual has the right to request erasure of their data (as stipulated in detail in Article 17); in other words, people are given a "right to be forgotten". In addition, Article 82 specifies the right to receive compensation in case any of the above rights have been infringed[10].

These rights are unique in the world's national legislations and acknowledge, in effect, personal data as an individual possession with considerable value. One can argue that, for the first time in history, people are given direct power over the use of their identity and characteristics. GDPR considers that not only identity traits but also personal choices are protected items that belong exclusively to the individual. The repercussions of such a qualitative legal step are profound, also for XR applications that must ensure their individual users' rights.

(d) Data Governance

Another key feature of GDPR is its focus on the governance of data. This relates to the obligations of the Controller and Processor and is stipulated in Articles 24-34. This covers a wide area, including storage, security, pseudonymising, use of algorithms, risk assessment, record keeping, reporting, etc. Data protection measures must be designed in the development of business processes for products and services[11]. Data protection impact assessments must be undertaken in case of processing sensitive data, and prior approval from data protection authorities must be obtained prior to data collection. Moreover, records of personal data processing activities must be kept (for most businesses) and handed over when

[8] Article 15, GDPR
[9] Article 15, 3 GDPR
[10] Article 82,1 GDPR
[11] Article 25, GDPR

requested by authorities, while data breaches must be declared within 72 hours after becoming aware of it[12].

Overall, it is clear that GDPR has also strict rules for businesses that collect and process personal data. This is in addition to the obligations stipulated in the Data Governance Act and the Data Act[13]. GDPR is the cornerstone of personal data processing obligations for both DGA and DA. Finally, attention should also be given to Article 40 that stipulates processes for the creation of codes of conduct[14]. Since codes of conduct for the proper application of GDPR are promoted, it should be expected that such codes will be created for XR applications in the near future. The XR4Human project's own code of conduct for the ethical application and a human-centred XR is an excellent example of such efforts.

2. Applicability to XR

It is apparent from the above description that so long as personal data is gathered via XR devices and software, GDPR is fully applicable and obligatory for developers. This is irrespective of the setting the reason for data gathering, or the aim of the XR device use, e.g. for research, entertainment, surveillance, etc. As such, all the compliance requirements described above are in full force. In addition, tools potentially leading to personal identification can, and almost certainly will, be treated as entities falling under the GDPR legislation.

We can conclude that GDPR is a crucial legislation in the field of XR. This means that organisations and businesses that use XR devices are liable to penalties as stipulated in the legislation. This is, of course, true only in case personal data gathering takes place, but, since GDPR correctly does not distinguish between direct and indirect data gathering, it is highly probable that almost any use of XR involves data gathering per GDPR. The onus to prove otherwise lies with the developer, not the user.

One immediate concern for XR service providers in relation to personal data is that, under normal circumstances, they must ensure fulfilment of the GDPR obligations via the creation of a position of data protection officer[15]. The tasks of the data protection officer are to ensure compliance with the regulation and be the primary contact point of the organisation about personal data. Other relevant tasks are data risk assessments, awareness raising, training and cooperation with the supervisory authority[16]. What is unclear for XR developers is whether a data protection officer position is necessary for SMEs that do not process large-scale of data since the regulation is not well-defined on this issue.

Considering the above, we will now look at areas of GDPR that can be particularly challenging to XR technologies. This refers to gathering data from special categories, data based on additional legislation, and ensuring the right to be forgotten.

2.1. Special categories of data

The first issue that must be clarified is the processing of special categories of personal data. According to GDPR, special categories are categories of data that reveal the person's[17]:

[12] Article 33, GDPR
[13] See DGA and DA sections
[14] Article 40, GDPR
[15] Article 37, GDPR
[16] Article 39, GDPR
[17] Article 9, GDPR

Funded by the European Union

- racial or ethnic origin
- political opinions
- religion or philosophical beliefs
- trade union membership
- data concerning health
- sexual orientation or activity and
- genetic and biometric data for identifying the person.

The argument behind identifying special categories of personal data is that data merits specific protection because processing could significantly risk the individual's fundamental rights and freedoms. In effect, processing such data is prohibited unless an exception can be made.

2.1.1. <u>Challenges for XR applications</u>

Considering the significant focus that GDPR places on special categories of data and the difficulty of accumulating or processing such data, it is essential to identify whether XR technologies can be used to gather special categories of personal data. The quick answer would be yes. First and foremost, VR devices can gather data such as iris scans, fingerprints or gait structures that constitutes biometric data. Moreover, analysis of eye movements and individual choices can infer other special categories of data such as ethnic origin, religious or political opinion and sexual orientation. Finally, it is even plausible to infer health data from movement patterns and XR applications can do that very effectively.

While XR technologies are not usually designed to gather such data (unless, of course, are applications specifically used in health care), it is the onus on the developer to prove that special categories of personal data will not and, even more, cannot be gathered with their devices. The former should be taken at face value, as it refers to a promise of action that can be verified independently. The latter, though, poses a real complication since the standard XR devices can gather are special categories of personal data by default. In this case, regulatory uncertainty surrounding XR technologies must be addressed.

There are cases where special categories of data can be processed as part of the GDPR provisions. These are[18]:

- When the data subject has given his or her explicit consent for processing the personal data in question.
- When the processing is necessary to protect the vital interests of the data subject or another person if the data subject is physically or legally incapable of giving consent.
- When personal data is processed in the course of the legitimate activities of a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim and the processing is appropriately protected, such processing may only relate to members or former members of the body or to persons who have regular contact with it in connection with its purposes. Data may not be disclosed outside that body without the consent of the data subjects.
- When the processing relates to personal data which are manifestly made public by the data subject, such as by publishing them on the data subject's website.
- When the processing is necessary to establish, exercise or defend legal claims. Processing is also permitted whenever courts are acting in their judicial capacity.

The case of informed consent is the most common plausible case for processing special categories of personal data in the XR field. As with countless other examples of standard digital platform usage terms

[18] Article 9, GDPR

Funded by the European Union

and conditions, consent for processing personal data is part of the (always lengthy and never usually read) terms and conditions for use. We can therefore deduce that individual consent will also be asked for and obtained by providers of XR technologies. But the validity of the consent vis a vis special categories of personal data can be legally disputed as being against the data minimalism principle of GDPR. In general, there should be no reason that standard XR applications gather purposefully any special categories of personal data, but they might do so without intend.

The other cases do not seem to challenge XR technologies, except perhaps the "manifestly public" data case. Here, one could argue that the XR device provider can lawfully process special categories of personal data that can be deduced by the XR user through his/her public profile.

2.2. Gathering data based on additional legislations

Personal data belonging to special categories can be processed if an exception to the prohibition has been provided for in the GDPR, Union law, or in national legislation. In this case, it is essential to identify whether special categories data can be processed by virtue of the GDPR or whether processing will require separate legislation or agreements in addition to the GDPR.

In the following cases, processing is not possible by virtue of the GDPR alone but requires more specific regulations or other procedures[19]:

- When processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or MS law or a collective agreement under MS law. Measures for safeguarding the fundamental rights and benefits of the data subject must also be stipulated in this connection.
- When processing is necessary for reasons of substantial public interest based on Union or MS law. The regulations that permit processing shall be proportionate to the aim pursued and respect the essence of the right to data protection. Measures for safeguarding the fundamental rights and benefits of the data subject must also be stipulated in this connection.
- When processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on EU or MS law or pursuant to a contract with a health professional. Such processing requires that the data is only processed by a professional or person subject to a statutory obligation of secrecy.
- When processing is necessary for public interest in public health, on the basis of EU or MS law which also provides for measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the GDPR and based on Union or MS law. The regulations that permit processing shall be proportionate to the aim pursued and respect the essence of the right to data protection. Measures for safeguarding the fundamental rights and benefits of the data subject must also be stipulated in this connection.

[19] Article 9, GDPR

2.2.1. Challenges for XR applications

In these particular cases, there is a vast grey area of interpretation that has created considerable discussions[20]. Although GDPR requires a detailed argumentation for processing special categories data, much of this argumentation refers to other legislations that GDPR has no particular view on. In other words, it leaves a window open for the widespread gathering and processing of sensitive personal data, so long as the responsibility falls under a different legislative regime.

To complicate things further, a much discussed ruling of the CJEU confirmed that the disclosure of personal data, even if done according to the national legislation, but has the potential to indirectly give away a special category of personal data, should follow the EU GDPR provisions for special categories of personal data[21]. This leaves a grey area as to what personal data any organisation or commercial interest can gather under other legislations that do not contradict GDPR.

Although this issue refers to a broader problem in respect to GDPR and affects all types of means of data gathering and any relevant technology, XR technologies have particular penetrative abilities in the possibilities to gather special categories of data. As such, GDPR provisions can potentially go unnoticed, and any type of biometric, health, behavioural and opinion data can be gathered indirectly via XR devices without the user's knowledge.

There is no obvious amending action in this respect, except perhaps increasing awareness for users of XR applications. As with any other technology that could be used to gather personal data, the user must be aware of the many possibilities of data gathering and provide their individual consent accordingly. A point of particular concern here is the chance of gathering and processing special categories of data within the working environment for assessment purposes (e.g. indirect health data of workers for assessment purposes). Where XR is widely used in work and education, the potential for indirect individual impact is significant, regardless of national legislation permissiveness.

2.3. Ensuring the right to be forgotten

GDPR has introduced particular clauses to allow for individual choices after personal data have been collected and processed. The so-called "right to be forgotten" appears in Recitals 65 and 66 and in Article 17 of the GDPR which states: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay". The process should not exceed one month, although the controller must also take steps to verify that the person requesting the data erasure is the data subject[22].

This right adds to the rights of data subjects to be informed about what type of personal data has been gathered and for what purpose. It can therefore provide a combination of the "know first and decide to erase afterwards" decision tree. The right to be forgotten is not absolute, though, as it can be activated in case the data subject no longer consents to processing, in case there are significant errors within the data, or if they believe information is being stored unnecessarily. On the other hand, an organisation's right to process someone's data might override their right to be forgotten in case that:

[20] See for instance, https://www.politico.eu/article/gdpr-rules-europe-facebook-data-protection-privacy-general-data-protection-regulation-cambridge-analytica/; https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855

[21] See https://curia.europa.eu/juris/document/document.jsf?docid=263721&doclang=EN

[22] Article 17, GDPR

- The data is being used to exercise the right of freedom of expression and information.
- The data is being used to comply with a legal ruling or obligation.
- The data is being used to perform a task an organization's official authority.
- The data being processed is necessary for public health purposes and serves the public interest.
- The data being processed is necessary to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional subject to a legal obligation of professional secrecy.
- The data represents essential information that serves the public interest, scientific research, historical research, or statistical purposes and where erasure of the data would likely impair or halt progress towards the achievement that was the goal of the processing.
- The data is being used to establish a legal defence or to exercise other legal claims.

2.3.1. Challenges for XR applications

Although this issue relates to any type of personal data processing, it is perhaps one of the most significant aspects of the GDPR with far-reaching consequences. The right to be forgotten assumes a direct communication line between technology providers, platforms, and users. This is not a given or a plausible arrangement in the case of XR technologies, which usually involve a fragmented and opaque relationship between designer, service provider, and user.

XR applications gather an enormous amount of indirect personal data (via body movements, eye focus, voice, exchanges between users, etc.) that allows them to infer personal information from allegedly anonymised data. For instance, an anonymously recorded gait movement configuration can be combined with datasets that record voices and user exchanges to identify the individual user and some of his/her background that constitutes special categories of personal data (e.g. political opinion or sexual orientation). However a possible request by the user to have his/her gait moment recordings erased cannot be given as these are anonymised recordings. Overall, it is unclear how effectively the right to be forgotten can be applied to XR technologies since developers cannot readily identify individual data.

3.2. e-Privacy Directive

1. Overview of the regulation

1.1. Scope

The Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, known as **e-Privacy Directive**) was published on 12 July 2002.

The e-Privacy Directive deals with digital technologies and in particular with applications on digital communications. It is an EU-wide instrument that attempts to harmonise the national provisions for protecting the fundamental rights and freedoms of individuals in the digital age. In particular, the Directive covers the right to privacy and confidentiality concerning the accumulation and processing of personal data in electronic communications. It also deals with the movement of data and electronic communications equipment and services in the EU. In a sense, there is considerable overlap with the scope of the General Data Protection Regulation (GDPR). However, the e-Privacy Directive focuses on the area of communication, making it a unique contribution to the challenges faced by new technologies such as XR.

1.2. Subjects

The main subjects of the e-Privacy Directive are related to the security of services and the confidentiality of information. Security of services refers to electronic communications providers and their obligation to ensure the protection of data and inform individuals in case of security breaches. Confidentiality of information refers to prohibitions on accumulating and processing data unless certain exceptions are evident. The definition of electronic communication services was traditionally limited to telecommunications services (e.g. voice calls) and transmission services in networks used for broadcasting.[23] This definition has been expanded by the Directive 2018/1972, known as Electronic Communications Code ("**ECC**"), and now includes internet access services, non-traditional interpersonal communications services (e.g. instant messaging), and machine-to-machine (M2M) transmission services.[24] However, the extension of the e-Privacy Directive to these new categories relies on its application by MS,[25] being one of the reasons why a new e-Privacy Regulation has been proposed.[26]

Moreover, the e-Privacy Directive deals with the everyday functions of online communications, such as cookies, unsolicited emails, and the traffic of processed data. As such, the Directive has a direct impact on the day-to-day activities of most EU residents. For instance, the ubiquitous "cookie choices" that everyone using the internet is faced with is the result of the implementation of the e-Privacy Directive. In a more indirect but also very impactful manner, the Directive is responsible for the lack of overwhelming unsolicited communication (emails, calls, SMS, etc.) that is evident in the EU but evident in other parts of the world.

[23] Article 2(c), Directive 2002/21.
[24] Article 2(4), EECC.
[25] Fieldfisher, A Tale of Two Directives: the European Electronic Communications Code and the ePrivacy Directive
[26] See Section 2. below.

1.3. Main provisions

The main provision of the Directive is the security of services. Article 4 states that: "The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard the security of its services, if necessary in conjunction with the provider of the public communications network concerning network security. With regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented at least:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure,
- ensure the implementation of a security policy concerning the processing of personal data."

The Directive also clearly states that in case of a data breach, the provider must notify the authorities and the subscribers immediately while providing proof that the breach was not the result of inadequate implementation of security obligations. Provider auditing falls under the national authorities' jurisdiction and follows national recommendations.

The second main provision of the Directive is the confidentiality of communications. Article 5 states that: "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality."

This is a key aspect with diverse legal consequences, as it ensures that new information or access to already stored information can only be done with the explicit consent of the subscriber or user of the service. Exceptions can only be allowed with explicit legal decisions (e.g., in case of threats to national security).

Following the above, the Directive clarifies data traffic and retention issues. Article 6 states that: "Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1)."

Further clarifications in this provision attempt to provide timelines for data retention (e.g., for billing purposes) and information provided to public authorities. Again, informed consent is a prerequisite for providers' data retention practices.

Perhaps the directive's most obvious direct impact is related to its approach to unsolicited communication and the use of cookies. Article 13 states that "The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent."

This, in effect, prohibits the widespread marketing method of "cold calling," whereby massive, unfocused calling is used to advertise and sell products and services. Most EU citizens have experienced the discontinuation of such calls when the Directive was implemented in their national context. A similar effect has been evident with unsolicited emails, although the structure of internet communications makes implementation harder in this case. As with the other provisions, informed consent is the only route to the continuation of such marketing activities.

Cookies are dealt with in Recital 25 that: "…Where such devices, for instance, cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices to ensure that users are made aware of the information being placed on the terminal equipment they are using. Users should be able to refuse to have a cookie or similar device stored on their terminal equipment…"

Cookies are then falling under Article 5 (confidentiality of communications). The Directive does not provide clear guidelines on the manner of opting out of the Cookie policy of the provider, but it sets an opting in approach via informed consent. The effect of the implementation is this aspect of the Directive has been widespread, with everyone experiencing constant requests to accept cookie policies on the internet. However, the actual effectiveness of confidentiality is doubtful since information on cookies is only sometimes clear and opting out possibilities are cumbersome.

2. The e-Privacy Regulation

Since a Directive functions as a series of guidelines for national legislation, it cannot guarantee the execution of its aims and obligations. Soon after the e-Privacy Directive was agreed upon, the attempt to turn it into a European legislation commenced. What was termed the "Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (**e-Privacy Regulation**) has been in discussion since 2017. The e-Privacy Regulation was scheduled to come into force along with GDPR as a compliment, creating a full-force legislation on privacy, security and data processing in the digital world. However, it proved to be challenging to reach a consensus amongst the MS, and although GDPR came into force in 2018, the e-Privacy Regulation is still in the discussion and negotiation phase.

If and when the e-Privacy Regulation comes into force, it will directly affect XR applications. For instance, the Regulation covers more than conventional telecommunications services, such as Internet, telephone, or messaging services. Over-the-Top services (OTT) such as VoIP services (e.g. WhatsApp, Skype, Telegram, etc.), e-mail services, and M2M transmission services also fall within the scope of the e-Privacy Regulation, following the scope of the EECC. VoIP and the M2M communication services can be key XR communication services and therefore, directly impacted by the Regulation. The M2M communication is a particularly contentious point. It has been extensively argued for and against, and while the European Commission has included it in its draft e-Privacy Regulation, the European Parliament entirely deleted the M2M section from its draft.

Moreover, the e-Privacy Regulation applies to all entities providing services in the EU, regardless of their residence status, as with the GDPR. Severe financial penalties are foreseen in case of breaches of the Regulation. This is also in accordance with the GDPR stipulations. Overall, they are complimentary regulations since the GDPR provides a framework for activities involving personal data, and the e-Privacy Regulation will apply this framework to privacy in electronic communications. It is foreseen that if e-Privacy Regulations conflict with the GDPR in any way, e-Privacy will override the GDPR.

3. Applicability to XR

As the e-Privacy Directive focuses on digital communications and confidentiality of data, there is an indirect connection to XR technologies that will depend on the extension of the concept of electronic communication services – whether is kept traditional or extended to instant messaging applications under the EECC. If the latter definition is applied by an MS, exchanges between users (e.g. conversations between players) in an XR environment may be regulated by the e-Privacy Directive. This ambiguity will be resolved by the e-Privacy Regulation if adopted. In any case, XR services will need to meet the criteria of not being a "minor and purely ancillary feature to another service" to be considered an electronic communication service.[27] If applicable, XR providers will need to meet retention, security and traffic requirements under the e-Privacy Directive.

Another point of interest would be the use of cookies. Again, XR applications will inevitably use cookies for functional and marketing purposes. This can be especially true for providers that include hardware and software options and both other business services (e.g. Meta). In such cases, cookies shall be used upon the user's or subscriber's explicit consent to the service. The fact that XR devices can, in principle, collect special categories of personal data (e.g. biometrics) can complicate the use of cookies and shows a current gap in the Directive. The interplay between the e-Privacy Directive and GDPR has been unclear since the Directive came into force. This issue was meant to be clarified with the e-Privacy Regulation.

[27] Recital 17, EECC

3.3. Data Act

1. Overview of the regulation

1.1. Scope

The Regulation on Harmonized Rules on Fair Access to and Use of Data (known as the **Data Act**, or "**DA**") entered into force on January 11, 2024. The Data Act is a key component of the EU's data strategy, advancing the objectives of digital transformation and addressing the challenges that revolve around the use of data in the EU.

It offers a comprehensive cross-sectoral regulation that applies to all economic actors within the EU. The Data Act covers a broad spectrum of data types, including:

- Personal and Non-Personal Data
- Data from Connected Devices (Internet of Things)
- Industrial Data
- Cloud Data
- Public Sector Data
- Emergency Data

These do not represent strict categories of data since there are obvious overlaps. For instance, personal data can be found in many data types (emergency, public sector, etc.). The types of data in DA refers to different services that are based on data. It is evident that much data generated by these services are not easily accessible to users and there are often challenges in the portability of data created through products connected to the internet[28]. The DA aims to ameliorate these problems and enhance business innovation.

The Data Act emphasizes fair access to data while safeguarding user rights and ensuring the protection of personal data. It clarifies who can create value from data and under which conditions. Moreover, it enables a fair distribution of the value of data by establishing clear and equitable rules for accessing and using data and encourages participation from various actors, regardless of their size, in the data economy.

Regarding commerce, the Data Act addresses contractual imbalances that hinder equitable data sharing. It provides legal certainty for companies and consumers engaged in data generation, particularly within the Internet of Things framework.

Overall, the Data Act promotes data-driven innovation, stimulates a competitive data market, and makes data more accessible to all users, contributing to the establishment of an EU single market for data. It relates greatly to, and expands, the Data Governance Act that aims to make more data available and facilitate data sharing across sectors and EU countries[29].

1.2. Subjects

The Data Act regulates mainly commercial entities that use data to develop their business, such as:

[28] Recital 20, DA

[29] See DGA section for more details

- Manufacturers of connected products: This includes entities that produce connected products such as cars, smart-home devices, and medical devices that are placed on the market in the EU.
- Providers of related services: Entities offering services related to connected products. These services could be directly linked to the use or management of connected products.
- Users in the EU; Individuals or businesses using connected products or related services within the EU.

XR developers fall clearly under these business types. They develop connected products (e.g. VR devices), provide related services for these products and are situated within the EU, using EU citizens' data. In addition, the DA also creates certain key categories to address the many challenges in the use of data that it tries to deal with:

- Data sharing services; Services that facilitate data sharing between organizations, promoting interoperability and collaboration. The Data Act encourages the creation of data intermediaries to facilitate secure and efficient data exchange[30].
- Data altruism: This is data sharing for the public good. The Data Act encourages individuals and organisations to share data voluntarily for research, innovation, and societal benefits[31].
- Data trustees: Trustees act as custodians of data, ensuring its responsible use and protection. They play a crucial role in managing data on behalf of others, such as individuals or communities.
- Data portability services: Data portability allows users to transfer their data seamlessly between service providers.
- Data innovation spaces: Spaces that encourage collaboration and experimentation with data and provide a supportive environment for data-driven innovation, research, and development.

Non-compliance with the Data Act is punished in several ways, including administrative fines (that can be substantial), a percentage of global turnover (up to 10% of the global annual turnover of an organisation), individual compensation (individuals affected by non-compliance may seek compensation for damages resulting from data sharing violations), injunctions and remedies (e.g. stopping non-compliant behaviour, imposing data sharing, etc.)[32] The exact rules on penalties are left to member states to decide individually.

1.3. Main provisions

The key provisions of the Data Act cover a broad spectrum of data use for mainly commercial but also for non-commercial purposes:

- Data sharing services[33]; The Data Act establishes a framework for data sharing services providers. These providers act as intermediaries, facilitating data sharing between data holders and data users. They must ensure transparency, non-discrimination and fair access to data.

[30] Data intermediaries were introduced in the Data Governance Act, see DGA section
[31] The definition of Data Altruism is provided in the Data Governance Act, see DGA section
[32] Recital 109 and Article 40, DA
[33] See Chapter II Business to Consumer and Business to Business Data Sharing

Funded by the European Union

- Data altruism[34]; The Data Act encourages data altruism, where organisations voluntarily share data for the common good. It provides legal clarity and protection for those engaging in such practices.
- Data portability[35]; The Data Act strengthens data portability rights for individuals. Users can easily transfer their personal data from one service provider to another, promoting competition and user empowerment.
- Data intermediaries[36]; The Data Act defines data intermediaries and sets rules for their behaviour. These intermediaries play a role in data transactions and must adhere to transparency and fairness principles.
- Data access and use rules[37]; The Data Act outlines rules for data access and use, emphasising fairness, non-discrimination and transparency. It ensures that data is accessible to a wide range of users.
- Data monopolies and imbalances[38]; The Data Act aims to prevent data monopolies and address imbalances in data access. It promotes a level playing field for all actors in the data economy.
- Data governance boards[39]; The Data Act establishes data governance boards at the EU and national levels. These boards oversee data sharing, monitor compliance, and resolve disputes.
- High-value datasets[40]; The Data Act identifies high-value datasets (e.g., geospatial, environmental, and mobility data) that should be made available for innovation and public interest.
- Data quality and liability[41]; The Data Act addresses data quality and introduces liability provisions. Data providers must ensure accuracy, and users must handle data responsibly.

It is clear that the DA is attempting to create very comprehensive legislation on data governance in the EU. Some of the provisions, such as those related to data altruism and governance structures, are based directly on the DGA while being more specific in their description of roles, responsibilities, and extent of coverage. The full application of the DA will doubtless have strong impact on businesses that are based on extensive datasets, whether residing in the EU or elsewhere.

2. Applicability to XR

Since XR applications depend heavily on data processing to achieve full functionality and improve their effectiveness and outreach, the DA has a direct bearing on their development. As we have seen above, various aspects of the DA impact directly on the applicability of XR.

[34] Article 49 (a) , DA
[35] Articles 30, 35, DA
[36] Recitals (26), (30), and (33) , DA
[37] Articles 41, 44, DA
[38] Article 33, DA
[39] Recital (110), Article 42, DA
[40] Articles 14, 15, 21, DA
[41] Article 3, DA

The main aim of the DA is to increase fairness in the digital environment by enhancing data access and distribution. For XR developers, this means they can potentially access more data generated by connected products and services, including IoT devices. This broader access can lead to better insights into user profiles and enhance innovation in XR applications. The DA encourages data-driven innovation by fostering data-sharing across sectors. This can create advantages for XR developers as they can benefit by leveraging diverse data sources to enhance their applications, create more immersive experiences, and improve user interactions. Since the DA does not differentiate between the amount of data in its sharing arrangements, it can benefit smaller developers by allowing them access to data they wouldn't otherwise be able to acquire. On the other hand, Big-Tech companies still hold a great advantage by monopolising the data market with their exceptional global access. Although the DA is trying to create a level playing field in data access, it is doubtful that the first-mover advantage that the Big-Tech enjoys will be reversed in the foreseeable future. The DA does not provide timelines for data sharing, and the precautions that data intermediaries must take mean possible delays in data access for smaller players.

In addition, the DA puts a lot of emphasis on privacy and data security by creating significant obligations for data use and considerable punishments for breaches and misuse. XR developers must be aware of these aspects and adapt their businesses accordingly. This can result in substantial additional expenditure, particularly for smaller developers. Particular attention should be paid to the following aspects:

- Data protection principles; The Data Act reinforces existing data protection principles, such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity. Developers handling data must adhere to these principles to ensure privacy rights are respected.
- User consent; The Data Act emphasises informed consent. Developers must clearly explain how they collect, process, and use personal data. Users have the right to know what data is collected, for what purpose, and how long it will be retained.
- Data breach notification: The Data Act requires timely notifications from affected individuals and relevant authorities. Developers must report breaches within a specified timeframe.
- Cross-border data transfers: The Data Act provides a framework for cross-border data transfers within the EU and from the EU to third countries. Developers must ensure that data is adequately protected during international transfers.

These aspects of the DA overlap considerably with the General Data Protection Regulation[42]. Issues of privacy, consent, user rights, and notifications are well regulated under GDPR, which is already enforceable in the EU. In this manner, the DA does not introduce any changes to the GDPR applications. It works in tandem with it while focusing on data access and data governance issues. XR developers can benefit directly from the DA by ensuring the above aspects are dealt with correctly (e.g. by establishing a Data Protection Officer position, as per GDPR) while working together with the data governance board of the DA to ensure fair access to datasets.

3. Data Act and AI Act

The relationship between the Data Act and the AI Act is important as big data is in the heart of both acts, but neither is straightforward in terms of the use of personal data. Although the Data Act specifically upholds and prioritises GDPR obligations in relation to personal data, there is considerable unclarity when

[42] See GDPR section

it comes to implementation. For instance, the DA states that[43]: "Third parties should also refrain from using data falling within the scope of this Regulation to profile individuals unless such processing activities are strictly necessary to provide the service requested by the user, including in the context of automated decision-making. The requirement to erase data when no longer required for the purpose agreed with the user, unless otherwise agreed concerning non-personal data, complements the data subject's right to erasure under Article 17 of Regulation (EU) 2016/679."

The interpretation of this is that AI systems can operate freely within the bounds of the DA, while the right to erase data is upheld via GDPR that, as we have seen, is ineffective in relation to current AI developments[44]. The right to be informed about one's personal data held in the dataset and the subsequent right to erase this data is technically very difficult, to almost impossible, for most Large Language Models supporting AI developments[45]. XR developers must therefore consider the ramifications of such challenges that oblige them to work in a "grey area" of personal data usage. The DA attempts to resolve such issues with the establishment of Data Intermediaries but before these are established within a robust regulatory framework, developers must prepare accordingly[46].

[43] Recital (39), DA
[44] See AI Act section
[45] https://www.fieldfisher.com/en/insights/get-ready-to-address-data-subject-rights-requests
[46] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/

3.4. Data Governance Act

1. Overview of the regulation

1.1. Scope

The **Data Governance Act** (**DGA**) is a regulation introduced by the EU to create a framework that facilitates data sharing[47]. The proposal for the DGA was first announced within the 2020 European strategy for data with the key objectives to:

- Increase trust in data sharing.
- Strengthen mechanisms for data availability.
- Overcome technical obstacles to data reuse.
- Support the setup and development of Common European Data Spaces in strategic domains (e.g., health, environment, energy, agriculture, mobility, finance, manufacturing, public administration, and skills)

The DGA entered into force on 23 June 2022 and following a 15-month grace period, it became fully applicable from 24 September 2023. The DGA lays down[48]:

(a) conditions for the re-use, within the EU, of specific categories of data held by public sector bodies;
(b) a notification and supervisory framework for the provision of data intermediation services;
(c) a framework for voluntary registration of entities which collect and process data made available for altruistic purposes; and
(d) a framework for the establishment of a European Data Innovation Board.

The DGA seeks to make more data available and facilitate data sharing across various domains, to increase benefits for European citizens and businesses. The prospective development of Common European Data Spaces involves private and public players to foster collaboration and data sharing within specific domains.

The DGA focuses on data management that can benefit industries and innovation. It assumes that good data management and sharing will help the development of innovative products and services, make the economy more efficient and sustainable, and benefit individuals by improving treatments and healthcare. For the latter, DGA foresees the establishment of mechanisms to facilitate the reuse of certain public sector data that cannot be made available as open data, such as, health data to advance research and find cures for rare or chronic diseases[49].

1.2. Subjects

The main areas that are regulated by the DGA cover the following:

- Re-use of certain categories of protected data held by public sector bodies
- Requirements applicable to data intermediation services
- Data altruism
- Competent authorities and procedural provisions

[47] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767
[48] Article 1, DGA
[49] Recital (3), DGA

- European Data Innovation Board
- International access and transfer

An essential aspect of the DGA is the introduction of the term "data altruism" which has significant ramifications for the regulatory status of this data. Its definition is given as[50]: "'Data altruism' means the voluntary sharing of data based on the consent of data subjects to process personal data about them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest;"

With the establishment of this new concept of data sharing, DGA attempts to develop possibilities for the creation of open data, amongst mainly public authorities, to improve services for citizens. It remains to be seen how far "data altruism" will be adopted and used for non-profit purposes in the EU. In any case, this aspect of the DGA fits very well the efforts of the European Commission to promote Open Science within its borders and beyond[51].

In terms of penalties, the DGA does not prescribe specific fixed penalties for non-compliance. Instead, it places the responsibility on MS to establish appropriate sanctions, fines, and penalties for infringements of the act[52]. Accordingly, these penalties must be effective, proportionate, and dissuasive. Basically, each MS can determine the specific consequences for violating the provisions of the DGA.

1.3. Main provisions

The main concepts that DGA attempts to regulate are:

- Data intermediaries; As entities that facilitate data sharing between data holders and users, the DGA introduces obligations for data intermediaries to adhere to transparency requirements, ensure data security, and act in the best interest of data subjects.
- Data altruism: Organizations that engage in data altruism (i.e., using and sharing data for altruistic purposes) must follow guidelines for secure data sharing, privacy protection, and ethical data handling.
- Technical measures; DGA emphasizes the use of technical measures to protect data privacy during reuse. These include techniques like anonymization, pseudonymisation and secure processing environments.
- European Data Innovation Board (EDIB): Established by DGA, the EDIB plays a central role in shaping data governance policies by providing guidance, monitoring compliance, and fostering innovation in data sharing.

Moreover, the DGA establishes several rights for users in terms of[53]:

- Data re-use; DGA grants users the right to access and reuse publicly held data. Users can request access to data held by public sector bodies and certain private entities.

---

[50] Articles 2, 16 DGA
[51] https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en
[52] Recital (55), DGA
[53] Recital (5), DGA

- Transparency and fairness; Data subjects have the right to transparent information about data sharing. For this reason, data intermediaries must act impartially and protect users' rights.
- Data portability: Users can request their data from data intermediaries to promote data mobility and empower individuals to switch between services.
- Redress mechanisms; DGA establishes mechanisms for resolving disputes related to data sharing, meaning that users can seek redress if their rights are violated.

2. Applicability to XR

The scope of DGA is very wide and applies broadly to all sectors of the economy that use data, meaning that it inevitably impacts XR developments as well. Its provisions cover all aspects of XR from manufacturers of connected devices (such as VR headsets), providers of related services, and users of such devices and services. It should be highlighted that when it comes to XR, DGA should be seen in relation to the subsequent Data Act, whereby both Acts interplay in issues of data use, processing and sharing[54]. It is not easy to differentiate between DGA and DA when it comes to impact on XR applications since both acts are equally valid in this case. DGA can be seen as a facilitator of data exchanges between the public sector and companies, while DA is the regulator. The biggest difference is the regulatory applicability of the acts, whereby DA is enshrined in the European regulatory regimes and contains specific obligations, non-compliance with, being punished with specific penalties.

The value of DGA in terms of companies that develop XR applications is in terms of data sharing, where DGA aims to democratise data access by making data available to small and medium-sized enterprises, startups, and individual consumers. XR developers may share data generated by their applications in order to expand the possibilities of immersion and user-friendly services. All big VR developers, such as Meta Platforms, Microsoft, Alphabet, Samsung, etc., incorporate connected devices and related services that fall under the auspices of DGA. In such cases, compliance with data sharing obligations would be beneficial and impact directly internal business processes.

Another key aspect of the DGA for XR developers is the establishment of data intermediation services. As data intermediation services are acting as trusted parties that facilitate the exchange of data between data holders and data users, they provide a neutral, transparent and secure environment that can benefit XR developers. Through the use of data intermediation service providers, businesses can get access to valuable data sets, including public sector data, that can be used to enhance the realism of their applications and improve user experience. Such datasets could derive from a wide range of activities such as healthcare, education and manufacturing. At the same time, the use of these datasets will imply full compliance with data protection laws, a fact that will enhance user trust in the application.

DGA provisions are not legally binding and there are no punishments for not following them. Each MS can establish national rules based on DGA and introduce penalties for infringements. It should be noted though that DGA attempts to enhance transparency and privacy in the use of data. XR developers must be aware that the DGA mandates clear and transparent communication about data use, and data intermediaries are obliged to inform users about how their data is collected, used and shared. Users are given the right to access and modify or even erase their data, while data processors are encouraged to use secure processing environments and anonymisation techniques. This aspect of the DGA, along with the strong provisions of the General Data Protection Regulation[55], creates a particular regulatory context for XR developers that would require from them to set up specific services in terms of data sharing,

[54] See DA section

[55] See GDPR section, particularly the discussion on special categories of personal data

transparency and privacy. It is therefore advisable that XR developers establish voluntary guidelines to secure user privacy through clear communication, privacy controls, and information security standards.

Finally, the fact that XR technologies deal by default with personal data requires particular attention to the role of the European Data Innovation Board[56]. The EDIB has a broad remit and includes representatives from industry, research, civil society and other relevant stakeholders. It has mainly an advisory role to the European Commission but also issues guidelines for cross-sector data use and engages in technical discussions on standardisation and interoperability. Furthermore, it coordinates national policies on the implementation of DGA. XR developers should engage directly with the EDIB to acquire clarity on the operation of data intermediaries in their jurisdiction and the steps they need to undertake to ensure best practices in data use.

[56] Articles 29 and 30, DGA

4. Intellectual property

4.1. Directive on Copyright in the Digital Single Market

1. Overview of the regulation

1.1. Scope

Directive (EU) 2019/790 of The European Parliament and of The Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC (hereafter referred to as the **Directive on Copyright in the Digital Single Market** or the **CDSM Directive**) is an EU directive that is aimed towards addressing the legal uncertainty arising out of particular uses of copyright in the digital environment.[57] The CDSM Directive was published in the Journal of the European Union on the 17th of May 2019 and came into force on 6 June 2019 with MS having until 7 June 2021 to implement it into their national law.[58]

The CDSM Directive seeks to supplement the existing copyright framework[59] by providing rules to adapt certain exceptions and limitations to copyright use and related rights to digital and cross-border environments, as well as for measures to facilitate certain licensing practices regarding the dissemination of out-of-commerce works and other subject matter together with the online availability of audiovisual works on video-on-demand platforms, to ensure more comprehensive access to content.[60]

1.2. Subjects

While laying down the rules which aim to harmonise further EU law applicable to copyright and related rights in the framework of the internal market, the directive is noted to be applicable to the following categories of subjects:

- **Online Content-Sharing Service Providers (OCSSPs):** The directive acknowledges the proliferation of online content – sharing services that provide access to a large amount of copyright-protected content uploaded by their users have become a main source of access to content online. Online services are recognized as a means of providing wider access to cultural and creative works and offer great opportunities for cultural and creative industries to develop new business models.[61] It is

[57] Recital (3), CDSM Directive

[58] Copyright and related rights in the Digital Single Market (europa.eu)

[59] Accordingly, the CDSM Directive complements the rules applicable to the existing copyright regime as outlined in the following directives: Directive 96/9/EC on the Legal Protection of Databases; Directive 2000/31/EC on Electronic Commerce; Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (the 'InfoSoc Directive'); Directive 2006/115/EC on Rental Right and Lending Right and on Certain Rights Related to Copyright in the Field of Intellectual Property; Directive 2009/24/EC on the Legal Protection of Computer Programs; Directive 2012/28/EU on Certain Permitted Uses of Orphan Works; and Directive 2014/26/EU on Collective Management of Copyright and Related Rights and Multi-Territorial Licensing of Rights in Musical Works for Online Use in the Internal Market.

[60] Recital (3), CDSM Directive

[61] Recital (61), CDSM Directive

noted however, that certain providers of online services, such as non-commercial platforms (i.e. not-for-profit online encyclopaedias, educational and scientific repositories), open source software-developing and-sharing platforms, providers of electronic communications services (such as Internet Service Providers (ISPs) and over-the-top (OTT) communication services that encompass video streaming platforms with communication or live chat features)[62], online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not considered to be OCSSPs within the meaning of the CDSM Directive.[63]

- **Rightsholders:** The directive explicitly acknowledges the need to achieve a fair balance between the rights and interests of authors and other rightsholders (e.g. performers, music publishers) on the one hand, and of users on the other hand.[64] It has been emphasised that this can only be achieved when rightsholders remain free to choose the appropriate means of enabling beneficiaries to benefit from them.[65]
- **Users of copyright-protected works:** Reiterating the issues highlighted above concerning the applicability of the directive, it is noted that the legislation seeks to address the imbalance between users and authors of copyright with the intent to provide rules to adapt certain exceptions and limitations to copyright use and related rights to digital and cross-border environments. It thus follows that users of the works fall within the ambit of persons that are subject to the regulations.

The CDSM Directive's territorial scope primarily focuses on services and providers established within the European Union. However, the Directive also has an extraterritorial reach, extending to businesses and platforms without an EU establishment that demonstrably targets their services to EU markets. This extraterritorial application could be determined by factors such as the service's accessibility within the EU, use of EU languages, payment in EU currencies, targeted advertising in the EU, or having a significant number of EU-based users.

1.3. Main provisions

The CDSM Directive aims to address various aspects of copyright law in the digital and cross-border context.[66] It includes provisions to adapt exceptions and limitations to suit digital environments, improve licensing practices for more comprehensive content access, and establish a fair marketplace for copyright.[67] Specifically, it introduces mandatory exceptions for text and data mining, digital teaching activities, and preservation of cultural heritage.[68] It also aims to facilitate access to out-of-commerce works, enhance collective licensing, and ensure availability of audiovisual content on online platforms.[69] Additionally, it introduces a related right for press publishers and mandates fair remuneration for authors and performers in exploitation contracts.[70]

Notably, the Directive introduces the following key provisions.

[62] Article 2 ,TRIPS Directive
[63] Article 2(6), CDSM Directive
[64] Recital (6), CDSM Directive
[65] Recital (7), CDSM Directive
[66] WIPO, Copyright in the Digital Single Market: a taster (wipo.int)
[67] Ibid.
[68] Ibid.
[69] Ibid.
[70] Ibid.

(a) Articles 3 and 4 provide two exceptions to copyright (and database right) infringement for text and data mining. The first is in relation to scientific research with rightsholders permitted to apply measures to ensure the security and integrity of the networks and databases where the works or other subject matter are hosted. However, the aforementioned measures shall not go beyond what is necessary to achieve that objective.[71] The second allows those with lawful access to the work to conduct text and data mining so long as it has not been expressly reserved (by the rightsholder) and the copies are only kept as long as necessary.[72]

(b) Article 17 introduces new obligations for OCSSPs. It makes OCSSPs directly liable if their users post unauthorised copyright material on their platforms. In order to avoid liability, OCSSPs will need to demonstrate that they have made "best efforts" to obtain permission from rightsholders (i.e. licenses), and acted diligently to remove any infringing content once notified by rightsholders (aka "notice and takedown"), as well as keep it disabled and thus prevent future unauthorised uses[73] (aka "notice and staydown").[74]

(c) Article 18 introduces the principle of appropriate and proportionate remuneration ensuring that authors and performers receive fair payment for the exploitation of their works, strengthening their often weak bargaining position when licensing or transferring rights.[75] This provision requires MS to consider factors like the work's actual or potential economic value, the contribution of authors/performers, and any revenue generated in determining "appropriate and proportionate" remuneration.[76]

2. Applicability to XR

2.1. Subjects regulated within the XR ecosystem

(a) XR platform providers: Understanding whether an XR platform falls under the definition of an OCSSP is crucial for purposes of discerning whether the platform has potential liability for copyright infringements committed by users within its virtual spaces. For instance, the legal rights applicable to the protection of unique creations and innovations associated with video games is bound to evolve as the in line with the development of XR technologies. By definition, OCSSPs encompass providers of an information society service as envisioned in the Technical Regulations Information System Directive.[77] Accordingly, their provision of public access to a large amount of copyright-protected works places the companies offering the services at higher

[71] Article 3(3) CDSM Directive

[72] Article 4(3), CDSM Directive

[73] Article 17(4), CDSM Directive

[74] Spindler, G. (2019). The liability system of art. 17 DSMD and national implementation: contravening prohibition of general monitoring duties. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10(3), 344-374.

[75] Article 18(1), CDSM Directive

[76] Article 18(2), CDSM Directive

[77] Article 1(1), TRIPS Directive

levels of risk should they unsuccessfully implement upload-filters as it is only in exceptional situations that CSSPs will not be required to use these filters.[78]

(b) XR users: The immersive nature of XR further complicates assessing whether content qualifies as user-generated or if the platform itself has a more significant role in creation and curation. Individuals creating XR-specific assets are entitled to the protections afforded by the CDSM Directive. Accordingly, expanding the scope of existing fair remuneration practices will be especially important, given the potential for collaboration and multi-layered contributions within XR works.

2.2. Challenges

(a) Liability and enforcement: Platforms recognised as OCSSPs where pre-existing copyrighted assets (3D models, music, code, etc.) are uploaded and shared by users will be required to incorporate more extensive filtering technologies under Article 17 CDSM Directive. As noted by the Committee on Legal Affairs of the European Parliament, "further clarification is needed on how existing rules should apply to online content-sharing services that make content available in virtual worlds and how they should be enforced".[79] As Lemley and Volokh point out, when an AR application applies filters which change the appearance of copyright works, or visually overlays and combines a copyright work with another protected work physically before a user, it creates a potentially infringing derivative work.[80] XR providers may need to be able to identify that an apparently new creation is actually a derivative of an existing work. The unique nature of XR environments challenges the straightforward application of traditional OCSSP liability. Accordingly, determining infringement responsibility in interactions within XR spaces will require evolving legal interpretations.

(b) Licensing: XR providers that qualify as OCSSPs will also need to secure updated and appropriate licenses in order to deploy copyrighted content in their platforms in a way that respects rightsholders. In addition, XR providers must be transparent with users in the use of copyrighted works if they are covered by their respective licenses. This is particularly interesting when it comes to the offering of digital assets associated with a non-fungible token (NFT). NFTs do not grant or imply copyrights or any other intellectual property rights to the owner of the digital asset.[81] In fact, those digital assets may use copyrighted works which will need to be covered by a license, otherwise they would be copyright infractions.

(c) User-generated XR content: Many XR platforms allow users to create and share their own creations, such as effects or 'filters' in AR applications or entire scenarios in VR games. These examples of user-generated content (UGC) are subject to the rules on appropriate and proportionate remuneration to creators under Article 18 of the CDSM Directive. XR platforms may need to review their monetisation and licensing schemes, particularly on those platforms where UGC is fundamental to their services. Another issue relates to the possibility that UGC involves the re-use of existing copyrighted works. Whether exceptions and limitations will adequately

[78] Spoerri T, *On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market*, Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 10(2), 173-186

[79] Committee on Legal Affairs, Report on policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues, 2023/2062(INI), para. 25.

[80] Lemley M, Volokh E, *Law, Virtual Reality, and Augmented Reality*, 166 University of Pennsylvania Law Review, 166(5), (2018), 1112

[81] Committee on Legal Affairs, Op. cit., para. 26.

protect UGC in XR remains unclear, and emerging litigation and subsequent case law will play an essential role in clarifying the balance between copyright and user creativity in evolving XR environments.

4.2. Regulation on the EU Trademarks

1. Overview of the regulation

1.1. Scope

Regulation (EU) 2017/1001 of the European Parliament and of the Council on the European Union trademark (hereafter referred to as the **Regulation on EU Trademarks Regulation** or the **Trademark Regulation**) was published in the Official Journal of the European Union on 14 June 2017. It came into force on 1 October 2017,[82] repealing the previous legislation on trademarks within the European Union, Council Regulation (EC) No 207/2009 of 26 February 2009 on the Community trade mark.[83]

One of the Trademark Regulation's objectives is to provide for Union arrangements for trademarks whereby undertakings can by means of one procedural system obtain EU trademarks to which uniform protection is given and which produce their effects throughout the entire area of the EU.[84] However, the legislation is careful to explicitly state that it does not replace the laws of the MS on trademarks and notes that it would not in fact appear to be justified to require undertakings to apply for registration of their trademarks as EU trademarks.[85]

The Trademark Regulation notes the confusion arising out of the inability to identify the true origin of goods provided by a company when n a company uses the same or a similar sign as a trade name in such a way that a link is established between the company bearing the name and the goods or services coming from that company.[86] Resultantly, the Trademark Regulation seeks to ensure trademark protection an combating counterfeiting effectively and in line with the European Union's international obligations by providing an opportunity for the proprietor of an EU trademark to be entitled to prevent third parties from bringing goods, in the course of trade, into the EU without being released for free circulation there, where such goods come from third countries and bear without authorisation a trade mark which is identical or essentially identical with the EU trademark registered in respect of such goods.[87]

The Trademark Regulation goes on to state that the exclusive rights conferred by an EU trademark should not entitle the proprietor to prohibit the use of signs or indications by third parties which are used relatively and thus by honest practices in industrial and commercial matters.[88] Further, in adherence to the principle of free movement of goods that it is essential that the proprietor of an EU trademark not be entitled to prohibit its use by a third party in relation to goods which have been put into circulation in the EEA, under the trademark, by him or with his consent, save where there exist legitimate reasons for the proprietor to oppose further commercialisation of the goods.[89]

[82] Article 212, Trademark Regulation

[83] Article 211, Trademark Regulation

[84] Recital (4), Trademark Regulation

[85] Recital (7), Trademark Regulation

[86] Recital (13), Trademark Regulation

[87] Recital (15), Trademark Regulation

[88] Recital (21), Trademark Regulation

[89] Recital (22), Trademark Regulation

The Trademark Regulation mandates MS with the obligation to designate, having regard to their own national system, as limited a number as possible of national courts of first and second instance having jurisdiction in matters of infringement and validity of EU trademarks.[90]

With regard to the applicability of these judgements across the different MS, the Trademark Regulation underlines the essentiality for decisions regarding the validity and infringement of EU trademarks to have effect and cover the entire area of the EU, as this is the only way of preventing inconsistent decisions on the part of the courts and the European Union Intellectual Property Office (EUIPO) –which is responsible for trademark registration, examination, and enforcement–[91] and of ensuring that the unitary character of EU trademarks is not undermined.[92]

1.2. Subjects

The subjects of the Trademark Regulation are noted to be any natural or legal person (with the inclusion of authorities established under public law), both seeking trademark protection for their goods and services within the EU[93] and affected by the use and registration of these trademarks, including competitors seeking to avoid infringement and consumers relying on trademarks to identify products and services.[94]

1.3. Main provisions

(a) Definition of a valid EU trademark: Article 4 provides that an EU trademark may consist of any signs, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other undertakings; and being represented on the Register of European Union trademarks, in a manner which enables the competent authorities and the public to determine the clear and precise subject matter of the protection afforded to its proprietor.[95]

(b) Absolute grounds for refusal: Article 7 outlines the absolute grounds for refusal regarding the registration of trademarks. It stipulates that trademarks failing to meet the criteria of Article 4, those lacking distinctive character, or consisting solely of signs or indications indicating various aspects of goods or services, such as their kind, quality, or geographical origin, are ineligible for registration.[96] Additionally, trademarks exclusively comprising shapes or characteristics inherent to the goods, necessary for technical results, or conferring substantial value to the goods, are not permissible.[97]

This criteria then extends to encompass, trademarks contrary to public policy or morality, those likely to deceive the public regarding the nature or origin of goods or services, and those lacking

[90] Recital (31), Trademark Regulation
[91] Article 2(1), Trademark Regulation
[92] Recital (32), Trademark Regulation
[93] Article 5, Trademark Regulation
[94] Recital 3, Trademark Regulation
[95] Article 4, Trademark Regulation
[96] Article 7(1), Trademark Regulation
[97] Article 7(1)(c), Trademark Regulation

authorization from competent authorities, are subject to refusal.[98] The article also addresses the exclusion of trademarks under various circumstances, including Union legislation, national laws, or international agreements, such as those safeguarding designations of origin, geographical indications, traditional terms for wine, traditional specialties guaranteed, and earlier plant variety denominations protected by relevant legislation or agreements.[99]

(c) Relative grounds for refusal: Article 8 then proceeds to outline the relative grounds for refusal in trademark registration.[100] Firstly, it outlines that if the trademark applied for is identical or similar to an earlier (EU, national or international) trademark for identical or similar goods or services, there exists a likelihood of confusion among the public, including association with the earlier mark, leading to refusal of registration. This more or less converges to the criteria outlined in Article 7(1)(g).[101]

Additionally, registration may be refused if the applied-for trademark is identical or similar to an earlier trademark and its use would unfairly exploit or harm the reputation of the earlier mark.[102] Furthermore, opposition by an authorized person regarding designations of origin or geographical indications can lead to refusal if certain conditions are met under relevant Union or national legislation.[103]

(d) Rights conferred by an EU trademark:

- Article 9 discusses the rights conferred by an EU trademark and begins by granting exclusive rights to the proprietor, enabling them to prevent third parties from using identical or similar signs in connection with identical or similar goods/services without the consent of the proprietor, particularly where such use could lead to confusion or dilution of the mark's distinctive character or reputation.[104] This prohibition encompasses various acts such as affixing the sign to goods or their packaging, offering or marketing goods/services under the sign, importing/exporting goods under the sign, using the sign in trade/company names, business papers, advertising, and comparative advertising.[105] Additionally, the proprietor can prevent unauthorized third parties from bringing goods bearing identical trademarks into the EU. However, this entitlement may cease if evidence is presented during infringement proceedings that the proprietor isn't authorized to prevent the goods' placement in the market.[106]

- Article 10 extends the right to prohibit preparatory acts related to packaging or other means bearing the trademark if there's a risk of infringement. This includes affixing identical or similar signs to packaging or other means and offering/placing on the market, stocking, importing/exporting such items.[107]

- Article 11 states that the rights conferred by an EU trademark prevail against third parties from the publication date of the trademark registration. It allows for reasonable compensation for

[98] Article 7(1)(g), Trademark Regulation
[99] Article 7(1)(j), Trademark Regulation
[100] Article 8, Trademark Regulation
[101] Article 8(1)(b), Trademark Regulation
[102] Article 8(1)(b), Trademark Regulation
[103] Article 8(6), Trademark Regulation
[104] Article 9(2), Trademark Regulation
[105] Article 9(3), Trademark Regulation
[106] Article 9(4), Trademark Regulation
[107] Article 10, Trademark Regulation

Funded by the European Union

acts occurring after the publication of a trademark application but before registration, provided those acts would be prohibited post-registration.[108]

(e) Infringement actions and remedies: Articles 123 to 126 outline the jurisdiction of EU trademark courts and the procedures for handling disputes related to infringement and validity of EU trademarks.[109] Article 123 stipulates that MS must designate a limited number of national courts and tribunals to handle EU trademark matters and inform the European Commission of any changes regarding their constitution as soon as possible.[110] Article 126 specifies the extent of jurisdiction of EU trademark courts, stating that courts have jurisdiction over acts of infringement or threatened infringement within their respective territories and acts referred to in Article 11(2) committed within any MS. Additionally, courts with jurisdiction based on Article 125(5) have authority solely over acts committed or threatened within their own MS.[111]

2. Applicability to XR

2.1. Obligations to XR providers

As recognised by the Committee on Legal Affairs of the European Parliament, the Trademark Regulation is fully applicable to XR platforms. This means that XR providers may obtain the registration of their trademarks used in XR products or services, while they must have an authorisation by the titleholder of a registered trademark in order to use identical or similar signs in connection with identical or similar goods/services.

For the registration of trademarks that identifies products or services in XR platforms, the International Classification of Goods and Services (also known as the Nice Classification), which is administered by the World Intellectual Property Organization (WIPO), has included several classes of trademarks to be implemented in virtual environments (see Table 1).

Table 1. Indications in Nice Classification regarding virtual worlds.[112]
Class 9 • 090934 downloadable application software for virtual environments • 090935 downloadable computer software applications for minting non-fungible tokens [NFTs] • 090870 downloadable computer software for managing crypto asset transactions using blockchain technology • 090841 downloadable cryptographic keys for receiving and spending crypto assets • 090918 downloadable digital image files authenticated by non-fungible tokens [NFTs] • 090933 downloadable digital music files authenticated by non-fungible tokens [NFTs] • 090842 downloadable e-wallets • 090929 downloadable virtual clothing

108 Article 11, Trademark Regulation

109 Section 2, Trademark Regulation

110 Article 123, Trademark Regulation

111 Article 126, Trademark Regulation

112 International Classifications - IT Support Area (wipo.int)

Class 36

- 360128 e-wallet payment services
- 360124 electronic transfer of cryptocurrency
- 360129 financial exchange of crypto assets
- 360139 online banking services rendered in virtual environments

Class 41

- 410256 entertainment services provided in virtual environments
- 410253 providing online virtual guided tours
- 410255 simulated travel services provided in virtual environments for entertainment purposes

However, even with these developments, both registration and use of third-party trademarks present challenges, as it will be analysed in the next section.

2.2. Challenges

(a) **Territorial scope:** Addressing the provision in Article 9 of the Trademark Regulation, which grants proprietors the authority to prevent unauthorised importation of goods bearing identical trademarks into the EU, presents notable challenges within the metaverse. The fact that trademark registration is linked to a particular jurisdiction (e.g. EU or national) may become difficult for an XR provider to have effective control over their trademark at a global level. The blurred jurisdictional boundaries inherent in virtual environments necessitate the development of interoperable mechanisms to reconcile multi-jurisdictional legislation and systems (e.g. Madrid Protocol) and enforce trademark rights effectively. Achieving this would require collaboration among stakeholders to establish standardised protocols for addressing trademark infringements and resolving jurisdictional disputes across diverse virtual platforms. Moreover, ensuring the interoperability of legislation and leveraging technological solutions like blockchain and smart contracts are crucial steps toward creating a secure and equitable virtual ecosystem that respects intellectual property rights while fostering innovation in the XR space.

(b) **Dilution of a trademark's distinctive character and reputation:** In exploring the rights conferred by an EU trademark, as outlined in Article 9 of the Regulation, questions arise regarding the scope of these rights within the context of XR environments. Specifically, concerns emerge regarding the extent to which trademark owners in the physical world can actually enforce their exclusive rights to prevent third parties from using identical or similar signs in connection with goods or services within XR spaces. Of particular interest is the concept of dilution of the mark's distinctive character or reputation within these immersive digital environments. Questions arise as to whether the evaluation of dilution would consider the reputation of the trademark solely within the XR space or extend to its reputation outside of this domain. Considering the unique nature of XR technologies, which blend physical and virtual realities, and the potential for trademark use within these environments to impact consumer perceptions and brand recognition, clarifications are sought regarding the applicability and enforcement of trademark rights in this evolving landscape. Additionally, inquiries arise concerning the measures available to trademark owners to safeguard their brand identities and prevent dilution or confusion within XR spaces, while also ensuring fair competition and innovation in this emerging sector.

Funded by the European Union

(c) **Enforcement:** Enforcing trademark rights under Article 11 of the Trademark Regulation necessitates XR providers to take robust tracing mechanisms to identify parties engaging in trademark violations. Additionally, collaboration between stakeholders, including trademark owners, XR platform operators, and regulatory authorities, is essential to establish standardized procedures for IP tracing and enforcement within the XR ecosystem. In addition, the applicability of EU jurisdiction raises questions regarding acts of infringement perpetrated outside the EU. Determining what constitutes an act of infringement within the jurisdiction necessitates clarification, particularly in the context of the XR space, where virtual goods and interactions transcend geographical borders. Factors such as the location of the infringing party or the servers where the platform is hosted, the impact on the EU market, and the applicability of international treaties may influence the court's interpretation of jurisdictional boundaries. Resolving these issues requires a nuanced understanding of cross-border enforcement mechanisms and collaboration between legal experts, policymakers, and international stakeholders to ensure effective protection of trademark rights in the global XR landscape.

(d) **Intangibility of goods:** Article 10 of the Trademark Regulation extends the right to prohibit preparatory acts related to packaging or other means bearing the trademark, particularly in cases where there's a risk of infringement. This encompasses actions like affixing identical or similar signs to packaging or other means, as well as offering, placing on the market, stocking, importing, or exporting such items. However, when considering its application in the context of XR, where intangible goods, such as those created by mods (modifications), are prevalent, complexities arise. Mods often involve user-generated content or alterations to existing virtual environments, introducing challenges in identifying and regulating trademark usage. Questions emerge regarding the extent to which trademark owners can enforce their rights over virtual goods within the XR space, especially when these goods are intangible and constantly evolving due to user-driven modifications. Additionally, the enforcement of trademark rights in the context of mods may require innovative approaches and technological solutions to monitor and regulate trademark usage effectively while balancing the interests of trademark owners and the XR community's creative expression. Similar challenge it is posed by NFTs, which usually reference trademarks without permission.[113]

[113] Committee on Legal Affairs, Op. cit., para. 24.

4.3. Directive on the Protection of Trade Secrets

1. Overview of the regulation

1.1. Scope

Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure (hereafter referred to as the **Directive on the Protection of Trade Secrets** or the **TSD**)[114] was adopted by the European Parliament and Council on the 8th of June 2016[115], was published in the Official Journal of the European Union on the 15th of June 2016 and entered into force twenty days after its publication.

Not having a direct effect on MS, the TSD was required to be incorporated through the bringing into force of national laws, regulations and administrative provisions by 9 June 2018.[116] In so doing, MS were required to communicate the text of the measures incorporated to the European Commission.[117]

The TSD acknowledges the investments made by businesses and non-commercial research institutions in acquiring, developing and applying know-how and information which is the currency of the knowledge economy and provides a competitive advantage.[118] This investment in generating and applying intellectual capital is recognised by the TSD as a determining factor as regards their competitiveness and innovation-related performance in the market and therefore their returns on investment, which is the underlying motivation for business research and development.[119]

Scholars note that trade secrets can be leaked by employees with special knowledge when they leave the company or disclose trade secrets by photographing and storing documents.[120] The estimated damage caused by industrial espionage has been noted to amount to around 50 billion euros per year in Germany alone.[121]

Accordingly the TSD is aimed at protecting the know-how and business information, whether as a complement or as an alternative to intellectual property rights, allowing creators and innovators to derive profit from their creation or innovation which is particularly important for business competitiveness as well as for research and development, and innovation-related performance.[122]

The TSD acknowledges that the differences in the legal protection of trade secrets provided for by the MS imply that trade secrets do not enjoy an equivalent level of protection throughout the EU, thus leading

[114] Directive - 2016/943 - EN - EUR-Lex (europa.eu)
[115] https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/trade-secrets_en (accessed on 21st March 2024)
[116] Article 19, TSD
[117] Article 19, TSD
[118] Recital (1), TSD
[119] Recital (1), TSD
[120] Hoeren, T, ' The New EU Directive on the Protection of Trade Secrets and Its Implementation,' in Corrales CM, et al. *Legal Tech and the New Sharing Economy. Perspectives in Law, Business and Innovation*. Springer, Singapore, 2020, 209
[121] Hoeren, T, ' The New EU Directive on the Protection of Trade Secrets and Its Implementation,' 210
[122] Recital (2), TSD

to fragmentation of the internal market in this area and a weakening of the overall deterrent effect of the relevant rules applicable to the protection of trade secrets.[123]

Accordingly, the Directive acknowledges the necessity of providing for rules at the Union level to approximate the laws of the MS to ensure that there is a sufficient and consistent level of civil redress in the internal market in the event of unlawful acquisition, use or disclosure of a trade secret.[124] The TSD goes on to provide that the rules should be without prejudice to the possibility for MS of providing for more far-reaching protection against the unlawful acquisition, use or disclosure of trade secrets, as long as the safeguards explicitly provided for in this Directive concerning the protection of the interests of other parties are respected.[125]

In the interest of legal certainty, and considering that legitimate trade secret holders are expected to exercise a duty of care as regards the preservation of the confidentiality of their valuable trade secrets and the monitoring of their use, the TSD endorses the restriction of the possibility of initiating actions for the protection of trade secrets to a limited period, requiring national law to specify from when that period is to begin to run and under what circumstances that period is to be interrupted or suspended.[126] This is then seen in Article 8, which places the limitation of actions at 6 years.[127]

1.2. Subjects

The subjects of the regulation are noted to be:

(a) Trade secret holders (individuals or businesses): Trade secret holders are defined in the TSD as any natural or legal person that is lawfully controlling a trade secret.[128]

(b) Infringers: These parties are defined as any natural or legal person that unlawfully acquires or discloses a holders trade secret.[129]

1.3. Main provisions

The Directive seeks to establish a homogenous definition of a trade secret without restricting the subject matter to be protected against misappropriation.[130] The definition of a trade secret emerges in Article 2 which outlines the three requirements in order for a piece of information to fall within the TSD as a 'trade secret'.[131] The TSD requires that the information must be kept confidential, not generally known or readily accessible to individuals within relevant industry circles;[132] secondly, it must possess commercial value specifically because it is kept secret;[133] and thirdly, it must have been subject to reasonable measures aimed at maintaining its confidentiality.[134] These requirements highlight the significance of secrecy,

[123] Recital (8), TSD
[124] Recital (10), TSD
[125] Recital (10), TSD
[126] Recital (23), TSD
[127] Article 8(2), TSD
[128] Article 2(2), TSD
[129] Article 2(3), TSD
[130] Recital (14), TSD
[131] Article 2(1), TSD
[132] Article 2(1)(a), TSD
[133] Article 2(1)(b), TSD
[134] Article 2(1)(c), TSD

commercial value, and diligent efforts to protect the confidentiality of information for it to be classified as a trade secret under the TSD.

Article 4 of the TSD discusses unlawful acquisition, use or disclosure and requires MS to apply the measures, procedures and remedies provided for in this directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of their trade secrets.[135] The TSD explicitly states that the acquisition of a trade secret without the consent of the holder is considered unlawful when it comprises of unauthorised access, appropriation, copying, of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced.[136] This also applies to any other behaviour contrary to honest commercial practices constitutes unlawful acquisition of a trade secret.[137] Similarly, the use or disclosure of a trade secret is deemed unlawful if it has been acquired through illegal means or violates a confidentiality agreement, contractual arrangement, or any duty of non-disclosure or limited use regarding the trade secret.[138] Further, it is prohibited to acquire, use, or disclose a trade secret if it is known or should reasonably be known that the information was obtained unlawfully from another party who was themselves unlawfully using or disclosing the trade secret.[139]Under Article 12 of the TSD there are injunctions and corrective measures to be implemented in the pursuit of redress for trade secret holders noting that MS shall ensure that, where a judicial decision taken on the merits of the case finds that there has been unlawful acquisition, use or disclosure of a trade secret, the competent judicial authorities may order the cessation or prohibition of trade secret use or disclosure.[140]

Courts are also empowered to order the prohibition of producing or marketing of infringing goods, as well as the adoption of corrective actions regarding such goods.[141] These corrective actions may involve recalling infringing goods from the market, removing their infringing quality, or destroying them, ensuring the protection of the trade secret in question.[142] Additionally, the TSD mandates the destruction or surrender of documents, objects, materials, substances, or electronic files containing the trade secret.[143]

Article 14 explicitly requires MS to ensure that the competent judicial authorities order an infringer who knew or ought to have known to be engaging in unlawful acquisition, use or disclosure of a trade secret, pay the trade secret holder damages appropriate to the actual prejudice suffered as a result of the unlawful acquisition, use or disclosure of the trade secret.[144] The liability of employees towards their employers for the unlawful acquisition, use or disclosure of a trade secret of the employer is however limited where they act without intent.[145]

2. Applicability to XR

2.1. Subjects regulated within the XR ecosystem

[135] Article 4(1), TSD
[136] Article 4(2)(a), TSD
[137] Article 42(a), TSD
[138] Article 3, TSD
[139] Article 4, TSD
[140] Article 12(1)(a), TSD
[141] Article 12 (1)(c) TSD
[142] Article 12(2), TSD
[143] Article (1)(d), TSD
[144] Article 14(1), TSD
[145] Article 14(1), TSD

Within the XR ecosystem, various subjects will be regulated, including XR developers, creators and businesses utilising XR for confidential commercial activities. XR developers often hold valuable trade secrets such as proprietary algorithms, unique interaction models, and specialised training datasets, which are critical for maintaining a competitive edge in the market. Similarly, businesses leverage XR technologies for internal VR training,[146] AR prototyping, and other confidential applications. Demonstrably, trade secrets play a pivotal role in driving innovation and maintaining market advantage.

2.2. Obligations for XR providers

XR providers will be obligated to implement robust security measures to safeguard proprietary information from unauthorised access, use, or disclosure in order to meet the required duty of care as provided for in the TSD. This will entail adopting encryption, access controls, and monitoring mechanisms tailored to the unique characteristics of XR platforms.

Additionally, monitoring adherence to confidentiality agreements with partners, collaborators, and employees will be essential to prevent inadvertent leaks or breaches of sensitive information. Understanding what constitutes lawful reverse engineering within the XR context, or rather, the limits of said reverse engineering, will be crucial for navigating intellectual property laws while innovating and developing new XR solutions.

2.3. Challenges in the implementation to XR or gaps identified

Implementing trade secret protections in the XR domain presents several challenges and potential gaps. The concern regarding the potential for XR technologies to enable new forms of trade secret misappropriation for instance poses one of the more significant challenges. In addition to the same, recording and analysing experiences in secure XR environments will pose risks of unauthorised access or replication of proprietary content. Additionally, determining what constitutes "reasonable" protective measures within highly dynamic, evolving and complex XR systems presents a challenge. The rapidly evolving nature of XR technologies necessitates constant vigilance and adaptation of current security protocols with the capacity to address emerging threats effectively.

In addition to the foregoing, a balance needs to be established between the need for secrecy to protect trade secrets and the desire for transparency and openness, particularly concerning XR datasets and algorithms. Balancing these competing interests requires careful consideration and will involve developing industry standards or guidelines that promote responsible innovation while safeguarding intellectual property rights and ensuring transparency where appropriate.

[146] XR4Human, Policy Report, p. 17.

5. Consumer and competition law

5.1. Consumer Rights Directive

1. Overview of the Regulation

1.1. Scope

The Directive 2011/83/EU of the European Parliament and of the Council on Consumer Rights (**Consumer Rights Directive** or "**CRD**") was published in the Official Journal of the European Union on 22 November 2011 and came into force 20 days later with the objective of achieving a high level of consumer protection across the EU and to contribute towards the proper functioning of the internal market by approximating certain aspects of MS' laws, regulations and administrative provisions concerning contracts concluded between consumers and traders.[147]

The CRD governs sales contracts, which refers to any contract under which the trader transfers or undertakes to transfer ownership of goods to the consumer including any contract having its object as both goods and services (including a digital service to the consumer). An off-premises contract is defined as any contract between the trader and the consumer that is concluded in the simultaneous physical presence of the trader and the consumer and in a place that is not the business premise of the trader or which may be concluded on the business premises of the trader or through any means of distance communication immediately after the consumer was personally and individually addressed in a place which is not the business premises of the trader. These include transactions by phone, mail order, e-mail, Internet or, alternatively, on the consumer's doorstep or any other place away from the retailer's established place of business.

Among the services that are regulated by the CRD are digital services, which are defined as a service that allows the consumer to create, process store or access data in digital form, uploaded or a service that allows the sharing of data or any other interaction with data in digital form that is uploaded or created by the consumer or other users of the service.[148]

The CRD explicitly highlights its applicability to the supply of digital content that is not on a physical medium or a digital service to a consumer.[149] It covers situations where the consumer provides personal data (following the concept of the GDPR) to the trader.[150] However, it does not apply if the personal data is used solely to supply the digital content or service, or to meet legal requirements, and the trader does not use the data for any other purpose.[151]

1.2. Subjects

The CRD is aimed to protects consumers, which are defined as natural persons that are acting for purposes that are outside their trade, business, craft or profession.[152]

[147] Article 1, CRD
[148] Article 2(2), DCD
[149] Article 3(1a), CRD
[150] Article 3(1a), CRD
[151] Article 3(1a), CRD
[152] Article 2(1), CRD

Traders must comply with the obligations under the CRD. These are defined as natural persons or legal persons irrespective of whether publicly or privately owned, that are acting including, through any other person, in their name or on their behalf for purposes relating to trade, business, craft or profession in relation to acts covered by the directive.[153]

1.3. Main provisions

a. **Information requirements:** Articles 6 and 7 of the CRD require traders to provide consumers with clear and comprehensive information before concluding distance or off-premises contracts. Specifically, Article 6(1) states that the trader must provide information about "the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services."[154] Article 6a mandates that online marketplaces provide specific information before a consumer is bound by a distance contract. This includes "general information, made available in a specific section of the online interface that is directly and easily accessible from the page where the offers are presented, on the main parameters determining ranking" and whether the third party offering the goods, services, or digital content is a trader or not.[155]

b. **Right of withdrawal:** Article 9(1) provides that the consumer shall have a period of 14 days to withdraw from a distance or off-premises contract, without giving any reason, and without incurring any costs other than those provided for in Article 13(2) and Article 14 which respectively the rights and obligations of the trader and the consumer upon the exercise of the right to withdrawal.[156] This provision provides a safeguard against impulsive or regrettable purchases which safeguard still applies in spite of the omission of information on the right of withdrawal as provided for in Article 10 which specifies that if a trader fails to provide the required information on the right of withdrawal, the withdrawal period extends to 12 months from the end of the day of the conclusion of the contract or the day that the consumer acquires physical possession.[157]

   The right of withdrawal may either be exercised using the model withdrawal form as is set out in Annex I(B) of the CRD or by making any other unequivocal statement.[158] The effect of exercising this right of withdrawal is the termination of the obligations of both parties to perform or conclude the contract.[159]

   The CRD mandates that the trader to reimburse all payments received from the consumer, including delivery costs, within 14 days of being informed of the consumer's decision to withdraw.[160] On the other hand, the consumer must return the goods to the trader within 14 days of communicating their decision to withdraw.[161]

[153] Article 2(2), CRD
[154] Article 6(1)(a), CRD
[155] Article 6a(1)(a), CRD
[156] Article 9(1), CRD
[157] Article 10(1), CRD
[158] Article 11(1), CRD
[159] Article 12, CRD
[160] Article 13(1), CRD
[161] Article 14(1), CRD

Article 15(1) states that ancillary contracts are automatically terminated when the consumer exercises their right of withdrawal.[162] Finally, Article 16 outlines specific exceptions where the right of withdrawal does not apply.

The CJEU has underscores the importance of consumers being able to exercise their right of withdrawal without facing undue obstacles. Notably, the CJEU provides that the right to withdrawal is intended to offset the disadvantage for the consumer by granting an appropriate period for reflection during which he can examine and test the goods required.[163] At the same time, the CJEU provided that sealed goods which are note suitable for return due to health protection or hygiene reasons and which have been unsealed by the consumer after delivery do not fall within the right of withdrawal and that such withdrawal would fall out of the right of withdrawal.[164]

c. **Delivery:** Article 18(1) stipulates that the trader shall deliver the goods by transferring the physical possession or control of the goods to the consumer without undue delay and not later than 30 days from the conclusion of the contract.[165] Article 18(2) proceeds to grant the trader additional time for delivery as would be appropriate depending on the relevant circumstances and in the event that the trader fails to deliver the goods within the additional period of time, then the consumer will be entitled to terminate the contract.[166] Upon said termination, the trader shall without undue delay, reimburse all sums paid under the contract. [167]

2. Applicability to XR

2.1. Subjects

The CRD has been updated to address digital content and services, which are integral to XR technologies. The Directive 2019/2161 (Better Enforcement and Modernisation Directive) extends consumer protection to digital content, ensuring that consumers have rights similar to those for physical goods. This includes the right to remedies if the digital content is not as described or fails to function correctly. For XR technologies, this means that software updates, digital environments, and virtual goods must meet the standards promised at the point of sale, and consumers must have recourse if these standards are not met.

Further, the CRD applies to the transparent information requirements for XR products and services, particularly regarding data collection practices, privacy implications, as well as health and safety risks associated with immersive experiences. The provisions of the directive address the right of withdrawal for digital content and services specific to XR, including virtual goods and in-app purchases. It also covers fair contract terms for XR platforms and marketplaces, ensuring that consumers are not bound by unfair clauses related to data usage or liability. Additionally, the directive might extend to cover aspects of XR that blur the lines between physical and digital goods, such as AR products or MR services. Given the immersive nature of XR, the directive could also address issues of informed consent and clarity of information presented within virtual or augmented environments. Finally, it would likely include

[162] Article 15(1), CRD
[163] *slewo – schlafen leben wohnen GmbH v Sascha Ledowski*, C-681/17, par. 33
[164] *slewo – schlafen leben wohnen GmbH v Sascha Ledowski*, C-681/17, par. 39
[165] Article 18(1), CRD
[166] Article 18(2), CRD
[167] Article 18(3), CRD

provisions for clear pricing information and protection against hidden charges in XR ecosystems, particularly in relation to subscription-based services or microtransactions within virtual worlds.

2.2. Obligations to XR providers

a) **Information requirements and transparency:** One of the core principles of the CRD is ensuring that consumers receive clear and comprehensive information before entering into a contract. This is particularly relevant for XR technologies, where the complexity of the products and services can be high. The CJEU has emphasised the necessity for businesses to provide information in a clear and comprehensible manner.[168] Notably, the CJEU provides that the directive aims to provide a high level of consumer protection by ensuring that consumers are informed and secure in transactions with traders. In addition, consumer protection is enshrined in EU policies by Article 169 TFEU and Article 38 of the Charter.[169] Applying this to XR technologies, companies must ensure that consumers are fully informed about the nature of the XR product, including hardware specifications, software requirements, potential health risks, and data privacy implications. This transparency is crucial given the immersive and often invasive nature of XR experiences.

b) **Right of withdrawal:** Consumers of XR products and services should be able to return hardware and cancel software subscriptions easily if they find the product does not meet their expectations or technical requirements. However, for devices such as VR headsets that require direct body contact for purposes of use and operation, once the packaging is unsealed the goods are deprived of the guarantee in terms of health protection or hygiene and may no longer be able to be used by a third party and as a consequence may no longer be able to be sold again by the trader.[170] In such an instance, the user in exercising the right of withdrawal would be liable for the diminished value of goods resulting from handling other than that necessary in order to establish the nature, characteristics and functioning of the goods. Regarding exceptions for the exercise of this right, the most relevant for XR providers is Article 16(m), which states that withdrawal does not apply to "the supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumer's prior express consent and acknowledgment that they will lose their right of withdrawal."[171]

c) **Unfair contract terms:** The CJEU has determined that the average consumer refers to a 'reasonably well-informed and reasonably observant and circumspect consumer.'[172] Accordingly, for XR technologies, this principle would apply to terms and conditions related to the use of XR hardware and software. Companies must ensure that their contracts do not include clauses that unduly limit consumer rights, such as excessive limitations on liability, mandatory arbitration clauses, or restrictions on the use of purchased content. National courts are expected to scrutinize these terms to protect consumers, ensuring that they are not unfairly burdened by the terms of XR service agreements.

[168] *Walbusch Walter Busch GmbH & Co. KG v Zentrale zur Bekämpfung unlauteren Wettbewerbs Frankfurt am Main eV*, C-430/17
[169] *Walbusch Walter Busch GmbH & Co. KG v Zentrale zur Bekämpfung unlauteren Wettbewerbs Frankfurt am Main eV*, C-430/17, par 34
[170] *slewo – schlafen leben wohnen GmbH v Sascha Ledowski*, C-681/17, par. 38
[171] Article 16(m), CRD
[172] *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Amazon EU Sàrl*, Case C-649/17, par. 37

d) Data protection: While not directly addressed by the CRD, data protection and privacy are critical issues for XR technologies, given their potential for extensive data collection. The principles established in the *Planet49* case**,** where the CJEU emphasized that pre-ticked boxes do not constitute valid consent under the GDPR.[173] For XR, this implies that companies cannot assume blanket consent for data collection through default settings. Further, it was held that users must be given clear information about the duration of cookie operation and whether third parties have access to the data.[174] For XR, this principle would extend to informing users about the types of data collected (e.g., biometric, movement, environmental) and how long it's retained. In addition to the same, the CJEU clarified that consent requirements apply even if the information stored or accessed is not personal data.[175] This is particularly relevant for XR, where some collected data might not immediately seem "personal" but could become so when combined or analysed. Finally, the judgment stressed the importance of informing users about who will have access to their data.[176] In the XR context, this could apply to informing users about which third-party developers or services might access data collected through a platform. XR companies must provide clear, accessible information about how personal data will be used, stored, and shared, and ensure that consumers can easily access and control their data.

[173] *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V*, Case C-673/17, par. 55
[174] *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, Case C-673/17, par. 80
[175] *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, Case C-673/17, par. 69
[176] *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, Case C-673/17, par 77

Funded by the European Union

5.2. Digital Content Directive

1. Overview of the Regulation

1.1. Scope

The Directive 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services, commonly known as the **Digital Content Directive** (**DCD**), was published in the Official Journal of the European Union on 22 May 2019. It came into force 20 days later and MS were required to adopt and publish measures necessary to comply with the DCD by 1 July 2021.[177] These measures were required to be in force by the 1 January 2022 and a review of the applicability of the DCD was to be conducted by the European Commission not later than 12 June 2024.[178]

The primary objective of the DCD is twofold: to contribute to the proper functioning of the internal market while ensuring a high level of consumer protection.[179] It achieves this by establishing standard rules on specific requirements concerning contracts between traders and consumers for the supply of digital content or digital services.[180] This harmonization aims to reduce legal fragmentation across MS, thereby enhancing consumer confidence in cross-border digital transactions and providing businesses with a more predictable regulatory environment.[181]

The DCD's scope is broad, applying to any contract where a trader supplies digital content or digital services to a consumer.[182] This includes not only contracts where the consumer pays a monetary price but also those where the consumer provides personal data as consideration.[183] However, the DCD explicitly excludes situations where personal data is processed solely for supplying the digital content or service, or for the trader to comply with legal requirements.

The DCD carefully delineates its scope by explicitly listing several types of contracts and services that fall outside its purview. This exclusion serves to ensure that sectors with unique regulatory needs are managed under appropriate frameworks, maintaining a clear and effective regulatory environment. The Directive does not apply to contracts for services other than digital services, even if digital means are used in their production or delivery.[184] This distinction helps to maintain a clear boundary between traditional services and purely digital offerings. Some of the services not covered by the DCD are:

- Electronic communications services, as defined in the European Electronic Communications Code (EECC), with the notable exception of N-IICS[185], which includes messaging services, videoconferencing services and email services.

[177] Article 24(1), DCD
[178] Article 25, DCD
[179] Article 1, DCD
[180] Article 1, DCD
[181] Recital 86, DCD
[182] Article 3(1), DCD
[183] Article 3(1), DCD
[184] Article 3(5), DCD
[185] Article 2(7), EECC

Funded by the European Union

- Healthcare services, provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices.[186]
- Gambling services that involve wagering stakes with monetary value, including games of chance and those with elements of skill, are excluded.[187]
- Financial services, specifically "any service of a banking, credit, insurance, personal pension, investment or payment nature"[188]
- Software offered under free and open-source licenses, provided that the consumer doesn't pay a price and any personal data provided is used solely for improving the software's security, compatibility, or interoperability.[189]
- Digital content made available to the public through means other than signal transmission, such as digital cinematographic projections.[190]
- Digital content provided by public sector bodies of MS in accordance with the Public Sector Information Directive.[191]

Lastly, the DCD addresses bundled contracts that include both digital content or services and other goods or services. In such cases, the DCD applies only to the elements of the contract concerning the digital content or digital service.[192] This provision ensures that the Directive's protections extend to the digital aspects of bundled offerings while allowing other relevant regulations to govern the non-digital components.

1.2. Main provisions

The main provisions of the DCD start with Article 5, which outlines the supply of digital content or digital services. This article stipulates that the trader shall supply the digital content or service to the consumer without undue delay after the conclusion of the contract, unless the parties have agreed otherwise.[193]

The DCD addresses the conformity of digital content or digital services. It establishes that the trader shall supply digital content or a digital service that meets the requirements set out in the subsequent provisions of the Directive.[194] Digital content or services shall be of the description, quantity, quality, functionality, compatibility, interoperability, and other features as required by the contract.[195] The directive also sets out the objective criteria that the digital content or service must meet, such as fitness for purpose, possession of qualities and performance features standard for digital content or services of the same type, and supply with accessories and instructions as the consumer may reasonably expect.[196]

Article 9 addresses the incorrect integration of digital content or services. It holds the trader liable for any lack of conformity resulting from incorrect integration if the integration was performed by the trader

[186] Article 3, Directive 2011/24
[187] Article 3 (5) (d), DCD
[188] Article 2(b), Directive 2002/65
[189] Article 3(5)(f), DCD
[190] Article 3(5)(g), DCD
[191] Article 3(5)(h), DCD
[192] Article 3(6), DCD
[193] Article 5(1), DCD
[194] Article 6, DCD
[195] Article 7(a), DCD
[196] Article 8(1)(a), DCD

or under their responsibility, or if the consumer integrated the digital content or service incorrectly due to shortcomings in the integration instructions.[197] Article 10 deals with third-party rights, stating that when a restriction resulting from a violation of any right of a third party, particularly intellectual property rights, prevents or limits the use of the digital content or service, the consumer is entitled to the remedies for lack of conformity.[198]

The DCD continues addressing the liability of the trader for any failure to supply the digital content or digital service. It stipulates that the trader is liable if they fail to supply the digital content or service without undue delay after the conclusion of the contract.[199] This provision ensures that consumers have recourse if the trader does not fulfil their obligation to provide the agreed-upon digital content or service in a timely manner. Such obligation is particularly important in the context of digital goods and services, where immediate or near-immediate delivery is often expected.

Article 12 deals with the burden of proof in cases of lack of conformity. It establishes that for any lack of conformity that becomes apparent within one year from the time of supply, the burden of proof regarding conformity lies with the trader.[200] This means that if a consumer reports an issue within this timeframe, it is up to the trader to prove that the digital content or service was in conformity at the time of supply. This provision significantly strengthens consumer protection by shifting the onus onto the trader to demonstrate that their product or service met the required standards at the time of delivery.

The DCD establishes essential remedies to ensure the rights of the consumers of digital services:

- If the trader has failed to supply the digital content or digital service, the consumer has the right to request that the trader supply the content or service without undue delay.[201] If the trader fails to do so, the consumer is entitled to terminate the contract.
- In case of a lack of conformity, the consumer is entitled to have the digital content or digital service brought into conformity, to receive a proportionate reduction in price, or to terminate the contract.[202]
- Right to terminate the contract: It allows consumers to terminate the contract even for minor absences of conformity if the lack of conformity is such as to justify immediate termination.[203]

The DCD then proceeds to outline the rights and obligations of traders in the event of contract termination. Article 16 specifies that upon termination, the trader may prevent any further use of the digital content or digital service by the consumer, particularly by making it inaccessible or disabling the user account.[204] However, the trader must also comply with obligations under the GDPR regarding the use of any personal data provided by the consumer.[205] Additionally, the trader is not required to make available any content other than personal data that was provided or created by the consumer when using the digital content or service supplied by the trader, except when such content has no utility outside the context of the digital content or service, relates only to the consumer's activity, or has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts.[206] This

[197] Article 9(b), DCD
[198] Article 10, DCD
[199] Article 11(1), DCD
[200] Article 12(1), DCD
[201] Article 13(1), DCD
[202] Article 14(1), DCD
[203] Article 15 , DCD
[204] Article 16(1), DCD
[205] Article 16(2), DCD
[206] Article 16(3), DCD

provision balances the trader's right to protect their digital assets with the consumer's right to retrieve their personal data and content.

Article 19 addresses the modification of digital content or services in contracts where the trader is to supply or make available the digital content or service over a period. It outlines the conditions under which such modifications can be made and the consumer's rights in such situations.[207] Finally, Article 20 provides for the right of redress, allowing the trader who is liable to the consumer due to a failure to supply or a lack of conformity to pursue remedies against persons in previous links of the chain of transactions.[208]

2. Applicability to XR

The DCD's definition of digital content as "data produced and supplied in digital form" is particularly pertinent to XR technologies.[209] This would encompass 3D models, virtual environments, and interactive digital assets used in XR applications. Similarly, the directive's definition of digital services, which includes services allowing consumers to create, process, store, or access data in digital form, or to share or interact with data uploaded by the consumer or other users, is highly relevant to XR platforms and social VR applications.[210] The directive's focus on goods with digital elements is also significant for XR hardware. For instance, VR headsets or AR glasses that incorporate digital content or services in a way that the absence of the digital component would prevent the goods from performing their functions would fall under this category.

Therefore, the DCD will be relevant for both consumers and traders of digital content in the XR environment.

Moreover, the DCD's provisions on compatibility, functionality, and interoperability are crucial for XR technologies. Compatibility in this context might refer to an AR application's ability to function with specific smartphone models or operating systems. Functionality could encompass the features and capabilities of a VR environment, while interoperability might relate to the ability of different XR platforms to exchange data or allow users to move between virtual spaces.

The directive's application to situations where consumers provide personal data as payment is particularly relevant to many XR applications that operate on a freemium model or collect user data for personalization and service improvement. This could include social VR platforms or AR apps that use location data to provide contextual information.

[207] Article 19(2), DCD
[208] Article 20, DCD
[209] Article 2(1), DCD
[210] Article 2(2), DCD

5.3. General Product Safety Regulation

1. Overview

1.1. Scope

The Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, known as **General Product Safety Regulation** (**GPSR**) replaces the General Product Safety Directive (GPSD), and shall be applicable from 13 December 2024. The erstwhile GPSD set out provisions requiring consumer products to be safe and for market surveillance authorities of the MS to act against dangerous products. However, an update to this law has been long overdue, given that the GPSD does not adequately address innovations in consumer products. The GPSR has been introduced to address new technologies and online marketplaces, to ensure greater harmonisation within the EU regarding product safety and recall, and to better regulate food-imitating products.[211]

Under the GPSR, a 'product' is any item supplied or made available to consumers or is likely to be used by consumers, whether or not provided for consideration or whether the consumers intended to use it.[212] Barring certain specific exclusions set out in Art 2(2)[213], the GPSR is applicable to all products placed or made available to the market. This includes products that are new, used, repaired or reconditioned.[214] For products that have specific safety requirements under valid EU law, the GPSR's obligations are supplementary in nature and only apply to those aspects not covered by the requirements under the specific EU laws. Importantly, products offered for sale online are deemed to be placed on the EU market and fall within the scope of the GPSR if the offer for that product is targeted at consumers in the EU, i.e., if the relevant economic operator acts in one or more MS.[215] This provision expands the scope of the GPSR and aims to address the role of online marketplaces in terms of product safety.

1.2. Subjects

The GPSR primarily focuses on setting out obligations for 'economic operators', which include any manufacturer, importer, distributor, fulfilment service providers or any natural or legal persons manufacturing or making available products in the EU market which fall within the scope of this law.[216] As stated above, the GPSR regulates any product made available in the EU market, including through online marketplaces.

1.3. Main provisions

The key provisions of the GPSR include the following categories of obligations- (a) safety obligations, (b) economic operator obligations, and (c) online marketplace provider obligations.

[211] Recital 2, GPSR.
[212] Art 3(1), GPSR.
[213] The GPSR does not apply to medicinal products, food, feed, living plants and animals, animal by-products and derived products, plant protection products, equipment on which consumers ride or travel where that equipment is directly operated by a service provider within the context of a transport service provided to consumers and is not operated by the consumers themselves, aircraft and antiques.
[214] Art. 2(3), GPSR.
[215] Art. 4, GPSR.
[216]

(a) Safety obligations:

- Economic operators must only place 'safe' products on the market;
    - A product's safety is assessed by considering its characteristics, effects by or on other products if the product is typically used in connection with other products, packaging and labelling, and the types of consumers using it.
    - When required by the nature of the product, safety must also be assessed by considering the appropriate cybersecurity features necessary to protect the product from external influences that impact its safety;
    - Similarly, assessing products involving emerging technologies, including products with AI-enabled or similar functionalities.
- Products shall be presumed as conforming to the relevant European standards or national requirements;

(b) Economic operator obligations:

- Manufacturer obligations:
    - Manufacturers must design and manufacture products as per the safety requirements in the GPSR;
    - Prior to placing products on the market, manufacturers must conduct an internal risk analysis and mitigation process and maintain documentation regarding this process;
    - Manufacturers must ensure that products bear clearly visible identification elements, and must provide their contact details on the product or its packaging;
    - If the manufacturer is aware that their product is a 'dangerous product', they must take corrective action immediately, including withdrawal or recall, and notify consumers and relevant authorities as prescribed.
- Importer and distributor obligations: Other than obligations regarding the design and manufacture of products, the obligations of importers and distributors are materially similar to the obligations of manufacturers. However, importers are also required to ensure that the safety of imported products is not compromised during the storage or transport stages. Further, importers must maintain an internal register of complaints to track complaints, accidents and corrective actions taken.
- Economic operators must cooperate with market surveillance authorities;
- Economic operators making their products available through distance sales must provide their name, registered trademark and contact details, along with information on the product and any warning or safety information which must be affixed to the product or its packaging.
- For specific categories or types of products that may pose a serious risk to consumers' health and safety, the European Commission may create a system of traceability, which the relevant economic operators must adhere to.

(c) Online marketplace provider obligations:

- Designating a single point of contact for communications with market surveillance authorities;
- Designating a single point of contact for communications with consumers regarding product safety issues;
- Compliance with orders from market surveillance authorities to take down listings offering specific products deemed to be dangerous, disable access or to display an explicit warning for such products;
- Designing their online marketplaces in a manner that allows traders offering products to set out the information required to be disclosed as per the GPSR, including the name and

contact details of the manufacturer, information regarding the product and if relevant, warnings or safety information.

2. Applicability to XR

2.1. Subjects regulated in the XR ecosystems

The GPSR is primarily concerned with the safety of products made available in the EU market and is, as such, part of a larger set of laws that guarantee the rights of consumers in the EU. The GPSR has a non-exhaustive scope in regulating products made available to consumers in one or more MS in the EU, barring a few specific types of products.

In terms of the XR market, this would primarily involve regulating any types of XR Hardware, including headsets, handheld devices or other interconnected aspects of an XR-enabled product that is made available to consumers. Although the GPSR does not cover services, products made available to consumers in the context of providing services are included in the scope of this law.[217] This would include instances where XR-enabled services are provided at 'virtual reality' experience stores. Given that XR technology relies on interconnection with other devices, the GPSR's provisions regarding product safety to consider cybersecurity aspects are critical for preventing malicious actors from disrupting a consumer's XR experience.

The GPSR uses the overarching term 'economic operator' to include manufacturers, importers, distributors, and any other legal or natural person involved in making products available to the market. Accordingly, any entity providing XR Hardware, regardless of its geographical location, is required to adhere to the GPSR if it makes products available to consumers in the EU.

2.2. Obligations for XR providers

The GPSR requires products to be safe, which includes mitigating risks posed to consumers including health risks and environmental risks. In this regard, the GPSR notes that the safety assessment for products must consider the health risks posed by digitally interconnected devices, including mental health risks, particularly for vulnerable consumers such as children.[218] Given that the risks to physical and psychological health posed by XR devices have been discussed by WP 3.1 in great detail[219], the safety assessment obligations under the GPSR are relevant for XR product manufacturers, distributors and other providers. Similarly, the safety of XR products would include assessing its cybersecurity features to protect consumers from unwanted external influence, and assessing any learning or predictive functionalities in the XR product.[220]

In addition to the safety assessment, as economic operators, XR providers must comply with further obligations set out in Section 1.3 above. This includes assessing and mitigating risks, maintaining technical documentation for up to 10 years, ensuring that the consumer is given relevant information regarding the manufacturer, importer and distributors. Economic operators must also cooperate with market surveillance authorities as required by the GPSR. This cooperation includes the revitalized version of the Rapid Information Exchange, an EU-wide alert system to flag unsafe products established under

[217] Recital 17, GPSR.
[218] Recital 23, GPSR.
[219] XR4Human, Policy Report, p. 15.
[220] Art. 6(g) and 6(h), GPSR.

the GPSD. Under the GPSR, businesses can inform market surveillance authorities through the Safety Business Gateway.[221]

[221] Art 9(8)(c), Art. 10(2)(c), Art. 11(2) and Art. 12(4)(c), GPSR.

5.4. Unfair Commercial Practices Directive

1. **Overview of the Directive**

1.1. Scope

The current version of the **Unfair Commercial Practices Directive** ("**UCPD**")[222] was published in the Official Journal of the European Union on 18 December 2019 and entered into force on 7 January 2020.[223] The UCPD is addressed to MS and to Iceland, Liechtenstein and Norway as signatories of the Agreement on the EEA. The UCPD requires the same to adopt and publish measures necessary to comply with the directive by 28 November 2021.[224] These measures are required to have been applicable from 28 May 2022.[225]

The UCPD is based on the principle of complete harmonization to remove internal market barriers within the EEA and increase legal certainty for both the consumers and businesses while establishing a uniform regulatory framework for the harmonisation of national rules. Prior to the coming into force of the 2019 reform, the UCPD required MS not to adopt stricter rules than those provided for in the directive, unless the same is provided for by the UCPD itself. This restriction was not applicable to financial services and immovable property where it is noted that MS were at liberty to impose requirements that were more restrictive or prescriptive than the Directive in the field in which they approximated.[226] It thus follows that in those sectors, MS were permitted to impose rules that go beyond the provisions of the UCPD as long as they were compliant with other European legislation.

With the coming into force of the 2019 amendments, Article 3(5) of the UCPD is noted to permit MS to adopt additional provisions to protect the legitimate interests of consumers with regard to aggressive or misleading marketing or selling practices.[227] However, such provisions shall be proportional, non discriminatory and justified on grounds of consumer protection. Notably, the UCPD does not affect the possibility of MS to set rules regulating commercial practices for reasons of health, safety or environmental protection.

Accordingly, the purpose of the UCPD is stated to be contributing to the proper functioning of the internal market and achieving a high level of consumer protection by approximating the laws, regulations and administrative provisions of MS on unfair commercial practices harming consumers' economic interests.[228] Therefore, national rules that aim to protect the economic interests of consumers even where in conjunction with other interests fall within this scope.

Business-to-business (B2B) commercial practices do not fall within the scope of the UCPD as they are partly regulated under the Misleading and Comparative Advertising Directive 2006/114/EC of the European Parliament and of the Council.[229] Further, Directive (EU) 2019/633 on unfair trading practices regulates B2B relationships in the agricultural and food supply chain. MS may however extend, under their national laws, the protection granted under the UCPD to B2B commercial practices.[230] This position

[222] Original version was published as Directive 2005/29/EC; current version is Directive (EU) 2019/2161.
[223] Article 8, UCPD
[224] Article 7(1), UCPD
[225] Article 7(1), UCPD
[226] Article 3(9), UCPD
[227] Article 3(5), UCPD
[228] Article 1, UCPD
[229] UCPD Guidance Note, Page 7
[230] UCPD Guidance Note, Page 7

was reiterated by the CJEU, by saying that a national provision does not fall within the scope of the UCPD "if it aims solely, as argued by the referring court, at regulating relations between competitors and does not aim at protecting consumers."[231] Where national measures regulate a practice with the dual aim of protecting consumers and competitors, then the rules will fall within the scope of the UCPD.[232]

Regarding the distinction between consumers' and competitors' interests, the CJEU has argued that only national legislation relating to unfair commercial practices which harm 'only' competitors' economic interests or which relate to a transaction between traders is excluded from that scope of the UCPD which is not the case with national provisions refer expressly to the protection of consumers and not only to that of competitors and other market participants.'[233]

1.2. Subjects

The provisions of the UCPD reveal its applicability to consumers and traders as well as products which have been defined as any good or service, including immovable property, digital service and digital content as well as rights and obligations. Further, the UCPD applies to business-to-consumer (B2C) commercial practices which are defined as any acts, omissions or course of conduct or representations and commercial communications such as advertising and marketing by a trader that are directly connected with the promotion, sale or supply of a product to consumers.

Notably the UCPD singles out its applicability towards vulnerable consumers by providing that where specific characteristics such as age, physical or mental infirmity or credulity make consumers particularly susceptible to a commercial practice or to the underlying product and the economic behaviour only of such consumers is likely to be distorted by the practice in a way that the trader can reasonably foresee, it is appropriate to ensure that they are adequately protected by assessing the practice from the perspective of the average member of that group.[234]

In addition to the foregoing the Directive is also applicable to regulated professions defined as professional activities, access to which or the pursuit of which is conditional directly or indirectly upon the possession of specific professional qualifications pursuant to laws, regulations, or administrative provisions. The Directive further applies to online marketplaces which are referred to under the legislation as a service using software including a website, part of a website or an application operated by or on behalf of a trader, which allows consumers to conclude distance contracts with other traders and consumers.

1.3. Main provisions

The UCPD begins by defining unfair commercial practices as that which is contrary to the requirements of professional diligence and that additionally distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is

[231] Case C-126/11, *Inno NV v Unie van Zelfstandige Ondernemers VZW (UNIZO), Organisatie voor de Zelfstandige Modedetailhandel VZW (Mode Unie), Couture Albert BVBA*, 15 December 2011, para. 29.
[232] UCPD Guidance Note, p. 7
[233] Case C-304/08, *Zentrale zur Bekämpfung unlauteren Wettbewerbse V Plus Warenhandelsgesellschaft mbH*, 14 January 2010, para. 39
[234] Recital 19, UCPD

addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.[235]

This definition additionally encompasses commercial practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group.[236] This is without prejudice to the common and legitimate advertising practice of making exaggerated statements or statements which are not meant to be taken literally.[237]

Article 6 defines misleading commercial practices as that which contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct in relation to one or more elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise.[238] Further, a commercial practice shall also be regarded as misleading if, in its factual context, taking account of all its features and circumstances, it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise and entails the marketing of a product that is inclusive of comparative advertising which creates confusion with any products, trademarks, names or distinguishing marks of a competitor.[239]

Article 7 discusses misleading omissions and provides that a commercial practice shall be regarded as misleading if, taking into account all of its features, circumstances and limitations of the communication medium, it omits material information that the average consumer requires according to the context to take an informed transactional decision and thereby cause or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.[240] This is also applicable to instances where a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information as referred to in that paragraph or fails to identify the commercial intent of the commercial practice if not already apparent from the context, and where, in either case, this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.[241]

Article 8 discusses aggressive commercial practices and provides that a commercial practice shall be regarded as aggressive where in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.[242]

Article 11 discusses enforcement and provides that MS shall ensure that adequate and effective means exist to combat unfair commercial practices in order to enforce compliance with the provision of the UCPD in the interest of the consumers.[243] These means shall include legal provisions under which persons or organizations under national law having a legitimate interest in combating unfair commercial practices

[235] Article 5(2), UCPD
[236] Article 5(3), UCPD
[237] Article 5(3), UCPD
[238] Article 6(1), UCPD
[239] Article 6(2), UCPD
[240] Article 7(1), UCPD
[241] Article 7(2), UCPD
[242] Article 8, UCPD
[243] Article 11(1), UCPD

may take the legal action necessary for the garnering recourse against such practices.[244] It shall be for each MS to decide which of these facilities shall be available and whether to enable the courts or administrative authorities to require prior recourse to other established means of dealing with complaints.[245]

Under Article 11a, consumers harmed by unfair commercial practices, shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract.[246] MS are required to determine the conditions for the application and effects of those remedies.[247] MS are also required to take into account, where appropriate, the gravity and nature of the unfair commercial practice, the damage suffered by the consumer and other relevant circumstances.[248]

Article 13 outlines the penalties applicable under the UCPD and provides that MS shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this directive and shall take all measures necessary to ensure that they are implemented.[249] In so doing, the prescribed penalties shall be effective, proportionate, and dissuasive.[250]

2. Applicability to XR

Advertising has been a critical driver for the digital economy, since it has promoted many organisational and technological innovations, and it has permeated the digital environment, contributing to expanding access to information.[251] In recent years, firms have been developing new forms of advertising based on XR technologies and, in particular, AR technology, in order to optimize and maximize sales.[252] This can be illustrated for instance through the Porsche AR visualizer which allows potential buyers to create a photorealistic representation of their configured vehicle in the real world and customise every single feature of the car before purchase.[253] In the highlighted form of advertising through the use of AR, the informative function consists in providing information to consumers about products, services and prices, allowing consumers to make reasoned choices about their purchases.

Accordingly, in the metaverse era, the customer journey will likely become more immersive and engaging.[254] As illustrated, the 3D nature of metaverse spaces gives customers a sense of presence, and conversely, as customers' avatars move through these 3D environments, more opportunities emerge for surveillance and monitoring of customers and their interests and preferences by observing, measuring, capturing, and analysing their actions for clues on how to engage with them more effectively.[255] Such practices could often be employed without the full knowledge of the consumer – it's possible these

[244] Article 11(1), UCPD
[245] Article 11(1)(b), UCPD
[246] Article 11a(1), UCPD
[247] Article 11a(1), UCPD
[248] Article 11a(1), UCPD
[249] Article 13(1), UCPD
[250] Article 13(1), UCPD
[251] Isola C, '*Augmented Reality, Advertising and Consumer Protection in the Light of European Union Law,*' Actualidad Jurídica Iberoamericana Nº 18, February 2023, 1489
[252] Ibid.
[253] New app makes three-dimensional vehicle configuration possible - Porsche Newsroom
[254] Marr, Bernard. *The Future Internet: How the Metaverse, Web 3.0, and Blockchain Will Transform Business and Society*. John Wiley & Sons, 2023, p 202
[255] Ibid.

commercial practices "may be manipulative" and, hence, unfair under consumer law and may also breach transparency obligations under data protection legislation.[256] These privacy concerns have, partialy, been addressed by the Digital Services Act (DSA), which mandates the explicit mention of restrictions on data usage, while the Digital Markets Act proposes the strict regulation of organisations providing core platform services if they qualify as 'gatekeepers.'[257]

The information paradigm suggests that when traders fulfil their obligation to provide information to consumers, the latter are sufficiently informed and therefore can make rational choices.[258] In turn, the consumers' ability to rationally locate products gives firms an incentive to compete to improve their offerings, including through relevant pricing methodologies.[259] For purposes of preventing market failures, different jurisdictions turn to legal and regulatory interventions, one of which is the requirement to disclose information.[260] Without such information, the incentive to compete on price and quality would be weakened, reducing consumer welfare.[261] Accordingly, the UCPD applies to XR through its regulation of the information that is provided to consumers.

This is further demonstrated through the requirement for Games studios which include promotions and advertisements in their games to ensure these are made sufficiently clear and are separate from gameplay, otherwise this could amount to a 'misleading practice'.[262] Further, when offering in-game purchases, traders must ensure they comply with information obligations under Article 7 UCPD and the Consumer Rights Directive. For example – the prices of virtual items should be clear and in fiat currency.[263]

With reference to the decision in *Wathelet v. Garage Bietheres*, the CJEU emphasizedthat the term "seller" must be interpreted in light of the objectives of the Consumer Sales Directive, which aims to provide high-level consumer protection.[264] The CJEU noted that while intermediaries are generally not considered sellers, they can be if they present themselves as the seller to the consumer.[265] Within the context of the metaverse and its regulation, this decision would apply to the interpretation of misleading actions under Article 6 of the UCPD. In particular, it would apply to the designs of marketplaces within the metaverses and the transparency with which they are presented to users of these technologies with a view towards ensuring that consumers are not misled about the identity of sellers in these marketplaces.

The regulation of XR technologies in the digital sphere will likely require a multi-faceted approach, combining elements from existing consumer protection frameworks. The UCPD, when considered in conjunction with the DSA, provides a foundation for addressing deceptive practices in virtual environments. However, the unique characteristics of immersive 3D worlds present novel challenges that may not be fully covered by current legislation.[266] As we venture into these new digital realms, we're likely

[256] New guidance for digital businesses on the Unfair Commercial Practices Directive - Wiggin LLP : Wiggin LLP
[257] Mitigating Risks for Effective User Privacy Protection in Metaverse (tcs.com)
[258] Beales, H., Craswell, R., Salop, S.C.: "The Efficient Regulation of Consumer Information", The Journal of Law and Economics, 1981, vol. 24, 534
[259] Ibid.
[260] Beales, H., Craswell, R., Salop, S.C.: "The Efficient Regulation of Consumer Information", 534
[261] Ibid.
[262] New guidance for digital businesses on the Unfair Commercial Practices Directive - Wiggin LLP : Wiggin LLP
[263] Ibid.
[264] *Sabrina Wathelet v. Garage Bietheres & Fils SPRL* (Case C-149/15), at par. 94
[265] *Sabrina Wathelet v. Garage Bietheres & Fils SPRL*
[266] Opinion piece: The DSA also works "in the metaverse" – if it is enforced well (interface-eu.org)

to encounter innovative forms of misleading design that go beyond traditional web-based deceptions.[267] To address these emerging issues, it's crucial that regulatory bodies take proactive steps. The European Commission, empowered by Article 25(3) of the DSA, has the authority to issue guidelines on deceptive design.[268] This provision offers a valuable opportunity to develop comprehensive standards that specifically target misleading practices in virtual 3D worlds.

[267] Ibid.

[268] Article 25(3), DSA

Funded by the European Union

6. Media and online services

6.1. Audiovisual Media Services Directive

1. Overview of the Regulation

1.1. Scope

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of specific provisions laid down by law, regulation or administrative action in MS concerning the provision of audiovisual media services (hereafter the **Audiovisual Media Services Directive** or **AVMSD**) aims to establish a comprehensive legal framework for content requirements across both linear and non-linear audiovisual media services, ensuring accountability among platform operators.[269] This involves encompassing new types of content, such as short video clips and user-generated content, where platform providers lack editorial responsibility, as well as including new providers explicitly.[270]

The AVMSD begins by defining an audio-visual media service as a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union.[271] The principal purpose of said service or a dissociable section thereof is devoted to providing programmes, under the editorial responsibility of a media service provider, to the general public in order to inform, entertain or educate by means of electronic communications networks within the meaning of the Framework Directive, 2002/21/EC.[272]

The AVMSD further defines a video-sharing platform service as a service provided by means of electronic communications networks where the principal purpose of the service or a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility and where the organisation of content provided is determined by the video-sharing platform provider by automatic means or algorithms and in particular by displaying tagging and sequencing.[273] The AVMSD goes on to refer to the term user-generated video as a set of moving images with or without sound constituting an individual item, irrespective of its length, which is created by a user and uploaded to a video-sharing platform by that user or any other user.[274]

To add to the foregoing, the term editorial decision under the AVMSD refers to a decision which is taken on a regular basis for the purpose of exercising editorial responsibility and is linked to the day-to-day operation of the audiovisual media service.[275] On the other hand, editorial responsibility refers to the exercise of effective control both over the selection of the programmes and over their organisation either in a chronological schedule, in the case of television broadcasts, or a catalogue, in the case of on-

[269] Report on the implementation of the revised Audiovisual Media Services Directive | A9-0139/2023 | European Parliament (europa.eu)
[270] Report on the implementation of the revised Audiovisual Media Services Directive | A9-0139/2023 | European Parliament (europa.eu)
[271] Article 1(a)(i), AVMSD
[272] Article 1(a)(i), AVMSD
[273] Article 1(aa), AVMSD
[274] Article 1(ba), AVMSD
[275] Article 1(bb), AVMSD

demand audiovisual media services.[276] Notably, editorial responsibility does not necessarily imply any legal liability under national law for the content or the services provided.[277]

1.2. Subjects

Under the AVMSD, the term media service provider refers to the natural or legal person who has editorial responsibility for the choice of the audiovisual content of the audiovisual media service and determines the manner in which it is organised.[278]

With regard to the definition of the term, 'broadcast,' it is noted that the provisions of the Directive only make reference to the term with reference to television broadcasts.[279] Put better, the Directive defines a broadcaster as a media service provider of television broadcasts which are in turn defined as audiovisual media services provided by a media service provider for simultaneous viewing of programmes on the basis of a programme schedule.[280]

So far, it is noted that the AVMSD restricts itself to definitions applicable to traditional media before accommodating technological developments through its definition of an on-demand audiovisual media service. According to the AVMSD, the same refers to an audiovisual media service provided by a media service provider for the viewing of programmes at the moment chosen by the user and at his individual request on the basis of a catalogue of programmes selected by the media service provider.[281]

The AVMSD is then noted provide definitions as would be applicable to marketing and advertising as is noted from the definition of 'audiovisual commercial communication' as images with or without sound that are designed to promote, directly or indirectly, the goods, services or image of a natural or legal person pursuing an economic activity.[282] It is expressly stated that the definition applies to images accompanying, or that include a programme or user-generated video in return for payment or for similar consideration or for self-promotional purposes. Forms of audiovisual commercial communication include, inter alia, television advertising, sponsorship, teleshopping and product placement.[283] Definitions under this category go on to encompass television advertising as well as surreptitious audiovisual commercial communication which entails broadcast for self-promotional services.[284]

The AVMSD further touches on marketing and advertising by providing a definition of 'sponsorship' as any contribution made by public or private undertakings or natural persons not engaged in providing audiovisual media services or video-sharing platform services or in producing audiovisual works to the financing of audiovisual media services, video-sharing platform services, user-generated videos or programmes with a view to promoting their name, trade mark, image, activities or products.[285]

---

[276] Article 1(c), AVMSD
[277] Article 1(c), AVMSD
[278] Article 1(d), AVMSD
[279] Article 1(e), AVMSD
[280] Article 1(f), AVMSD
[281] Article 1(g), AVMSD
[282] Article 1(h), AVMSD
[283] Article 1(h), AVMSD
[284] Article 1(i), AVMSD
[285] Article 1(k), AVMSD

1.3. Main provisions

(a) Criteria for the establishment of a Media Service Provider: In Article 2 of the AVMSD, it is noted that each MS shall ensure that all audiovisual media services transmitted by media service providers under its jurisdiction comply with the rules of the system of law applicable to audiovisual media services intended for the public in that MS.[286] Further, the Directive provides criteria for the evaluation of whether a media service provider is deemed to be established within a MS. The criteria takes into consideration factors such as the location of the provider's head office, where editorial decisions are made, and the presence of a significant part of the workforce involved in the audiovisual media service activity.[287] This criteria further expands to include media service providers that use a satellite up-link or satellite capacity appertaining to a particular MS.[288]

(b) Freedom of reception: In Article 3, it is expressly stated that MS shall ensure freedom of reception and shall not restrict retransmissions on their territory of audiovisual media services from other MS.[289] However, this freedom of reception is quantified to exclude instances where a media service provider contravenes the provisions of Article 6(1)(a) or Article 6a(1) of the AVMSD which pertains to the provision of services that contribute to the incitement to violence and hatred or the impairment of the physical, mental or moral development of minors respectively.[290] Harmful content such a gratuitous violence and pornography also fall under the exceptions to the freedom of reception. On the same tangent, the Directive restricts the collection or generation of personal data for minors by media service providers for purposes such as direct marketing, profiling and behaviourally targeted advertising.[291] The Directive then proceeds to task MS with ensuring that media service providers provide sufficient information to viewers about content which may impair the physical, mental or moral development of minors and that this information adheres to a standard system of describing the potentially harmful nature of the content of an audiovisual media service.[292]

(c) Marketing and advertisements: Under Article 9 pertaining to marketing and advertisements, it is noted that the AVMSD expressly states that MS are responsible for ensuring that audiovisual commercial communications provided by media service providers within their jurisdiction meet specific criteria.[293] These communications must be clearly identifiable as commercial content and cannot utilize covert techniques.[294] Media service providers are also prohibited from employing subliminal methods.[295] Additionally, such communications must uphold principles of respect for human dignity and refrain from promoting discrimination based on various grounds such as sex, race, ethnicity, nationality, religion, belief, disability, age, or sexual orientation.[296] The Directive additionally prevents media service providers from encouraging behaviours that pose risks to health or safety or advocating for actions

[286] Article 2(1), AVMSD
[287] Article 2(3), AVMSD
[288] Article 2(4), AVMSD
[289] Article 3(1), AVMSD
[290] Article 3(2), AVMSD
[291] Article 6a(2), AVMSD
[292] Article 6a(3), AVMSD
[293] Article 9(1), AVMSD
[294] Article 9(1)(a), AVMSD
[295] Article 9(1)(b), AVMSD
[296] Article 9(1)(c), AVMSD

that significantly harm environmental protection efforts.[297] Further, MS are mandated to prohibit all forms of audiovisual commercial communications related to cigarettes, tobacco products, electronic cigarettes, and refill containers.[298] Advertisements for alcoholic beverages are expressly required not to target minors specifically and should not encourage excessive consumption.[299] Finally, audiovisual commercial communications promoting medicinal products and medical treatments available only through prescription within the MS where the media service provider operates are forbidden.[300]

(d) Local content: With regard to the component of local content accessed video on-demand audiovisual media services, it is noted that Article 13 requires MS to ensure that media service providers of on-demand audiovisual media services under their jurisdiction secure at least a 30% share of European works in their catalogues and ensure prominence of those works.[301] Further, where media service providers are required by MS to make financial contributions towards the production of European works, the providers targeting audiences in other territories will also be required to make such contributions towards the production of the works as are proportionate and non-discriminatory.[302]

(e) Content moderation: Chapter IXA outlines the provisions that are particularly applicable to video-sharing platform services, beginning with Article 28b which requires MS to safeguard specific audiences from potentially harmful content.[303] This protection applies in three key areas. Firstly, it shields minors from programs, user-generated videos, and commercials that could negatively impact their physical, mental, or moral development.[304] This aligns with the principles outlined in Article 6a(1) as was previously discussed. Secondly, the general public is protected from programs, user-generated videos, and commercials that incite violence or hatred against specific groups based on characteristics outlined in Article 21 of the Charter of Fundamental Rights.[305] Finally, the Directive reiterates the need to shield audiences from programs, user-generated videos, and advertisements that promote criminal activity.[306] This includes content that publicly encourages terrorist acts (as outlined in Article 5 of the Anti-Terrorism Directive, child pornography offenses (as detailed in Article 5(4) of the Child Sexual Abuse Directive), and offenses related to racism and xenophobia (as defined in Article 1 of the Framework Decision on Racism and Xenophobia).[307]

(f) Video-sharing platform services: Through the introduction of codes of conduct applicable to video-sharing platform services, the AVMSD proceeds to require MS to encourage co-regulation and self-regulation aimed at significantly restricting advertisements for food and beverages high in nutrients and substances with a demonstrated negative health impact.[308] These substances include fat, trans-fatty acids, salt or sodium, and sugars, for which

[297] Article 9(1)(c)(iv), AVMSD
[298] Article 9(1)(d), AVMSD
[299] Article 9(1)(e), AVMSD
[300] Article 9(1)(f), AVMSD
[301] Article 13(1), AVMSD
[302] Article 13(2), AVMSD
[303] Article 28b(1), AVMSD
[304] Article 28b(1)(a), AVMSD
[305] Article 28b(1)(b), AVMSD
[306] Article 28b(1)(c), AVMSD
[307] Article 28b(1)(c), AVMSD
[308] Article 28b(1)(2), AVMSD

excessive consumption within the overall diet is expressly discouraged.[309] It is noted from the AVMSD that it shall be the obligation of MS to ensure that all video-sharing platform providers under their jurisdiction apply such measures as will be practicable and proportionate, taking into account the size of the video-sharing platform service and the nature of the service that is provided.[310] Further it is an express provision that the measures shall neither lead to any ex-ante control measures nor upload-filtering of content which do not comply with Article 15 of e-Commerce Directive.[311]

(g) **Alternative Dispute Resolution:** Forecasting the likelihood of disputes arising out the implementation of these provisions, the Directive proceeds to require that MS ensure the availability of alternative dispute resolution mechanisms for the settlement of disputes between users of platforms and the video-sharing platform providers.[312]

2. Applicability to XR

2.1. XR platforms subject to the regulation

Being technologically neutral, the AVMSD covers all audiovisual media services, regardless of the delivery technology used.[313] This accordingly encompasses both traditional and contemporary forms of media ranging from film, TV, digital media and video sharing to include XR and video games. This means the AVMSD is applicable to online platforms using VR, AR, and MR when they are used to provide audiovisual content. Accordingly, the evolution of the Directive to accommodate online streaming services and incorporate them within the purview of the legislation demonstrates the intent of the European Commission to be cognizant of changes in technology and the prospective impact on users.

Some XR experiences might fall within the scope of on-demand audiovisual media services as defined by the Directive. A platform that would for instance, offer curated collections of video through XR devices (e.g. YouTube VR) would fall within the scope of the Directive given that these experiences would be considered analogous to on-demand movies or television shows, potentially bringing them under the purview of the AVMSD.[314] To add on to the foregoing, the Directive's focus on video-sharing platforms offers a potential framework for regulating user-generated XR content. XR technology could enable the creation and sharing of immersive experiences – e.g., user-created VR tours or interactive games.

2.2. Challenges

The AVMSD's provisions regarding the protection of minors and the general public from harmful content, as well as its emphasis on co-regulation and self-regulation for video-sharing platforms imply that heightened obligations like prohibiting incitement to hatred, ensuring accessibility for disabled persons, and following rules on commercial communications would apply to XR audiovisual services.[315]

[309] Article 28b(1)(2), AVMSD
[310] Article 28b(1)(3), AVMSD
[311] Article 28b(1)(3), AVMSD
[312] Article 28b(1)(7), AVMSD
[313] General Principles of the AVMSD | Shaping Europe's digital future (europa.eu) (accessed on May 1, 2024)
[314] General Principles of the AVMSD
[315] General Principles of the AVMSD

With reference to our previous report on policy debates, it is noted that in addressing the social implications of XR technologies, child safety is at the forefront of the concerns surrounding the use of the internet and social media. Issues such as bullying, harassment or stalking, grooming, doxing and other forms of violence, threats, and abuse have been identified as prominent risks that children are exposed to.[316]

Such report further draws attention to the concern arising out of the continuing impact of the deployment of XR technologies in influencing public opinion as has been demonstrated in the Cambridge Analytica scandal, where social media bots were deployed in the manipulation of political opinion with a demonstrated effect on voting patterns.[317] The use of bots and deepfakes is likely to proliferate the XR sphere as the use of the technologies increases in reach and scale. Accordingly, this calls for the adaptation of the existing technologies to address the arising challenges prior to counter the possibilities of their abuse.

Due to the immersive nature of XR compared to traditional media, are estimated to have a larger impact on children as they continued to be scaled out to consumers, than if the same incidents occurred in traditional online environments.[318] Further, due to place and plausibility illusions, it is anticipated that the users of XR technologies will react realistically to the virtual reality that they are in.[319] This increases the vulnerability of the users of XR technologies to the content that will made available on the platforms, thereby making a stronger case for the development of more proactive content moderation mechanisms as the use of XR technologies.

[316] XR4Human, 'State-of-art in XR Policy Debates', p. 38
[317] XR4Human, 'State-of-art in XR Policy Debates', p. 39
[318] XR4Human, 'State-of-art in XR Policy Debates', p. 39
[319] XR4Human, 'State-of-art in XR Policy Debates', p. 39

6.2. Digital Services Act

1. Overview of the regulation

1.1. Scope

The Regulation (EU) 2022/2065 on a Single Market for Digital Services or **Digital Services Act** (**DSA**) is an EU regulation that establishes a responsibility regime for digital services that act as intermediaries. The DSA was published in the EU Official Journal on 19 October 2022 and enacted on 16 November 2022, replacing and expanding the liability regime contained in the E-Commerce Directive 2000/31/EC. It has been fully applicable since 17 February 2024.

The DSA aims for a 'safe, predictable and trustworthy online environment' that allows end-users to effectively protect and exercise their fundamental rights guaranteed in the EU Charter of Fundamental Rights. The DSA helps to achieve this goal by harmonising the rules for digital services and overcome the regulatory fragmentation generated by the implementation of the former E-Commerce Directive by MS.[320]

1.2. Subjects

The DSA regulates the provision of intermediary services in the internal market, by establishing a framework for the conditional exemption from liability of providers of intermediary services; rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services; and rules on its implementation and enforcement.[321]

The specific categories of intermediary services providers are the following:

(a) **Intermediary services** cover three different types of information society services: (i) **'mere conduit' services**, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network (e.g., VPN, top-level domain registries); (ii) **'caching' services**, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request (e.g., content delivery networks); and (iii) **'hosting' services**, consisting of the storage of information provided by, and at the request of, a recipient of the service (i.e., cloud services).[322] These are the categories previously regulated by the E-Commerce Directive

(b) **Online platforms** (**OPs**) are a subcategory of hosting services that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of the DSA (e.g., social media, online marketplaces).[323] A similar category of intermediary services are the **online search engines** (**OSEs**), which allow users to input queries in

[320] Recitals (3) and (4), DSA.
[321] Article 1(2), DSA.
[322] Article 3(g), DSA.
[323] Article 3(i), DSA.

order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.[324]

(c) **Very large online platforms** (**VLOPs**) are a subcategory of OPs which reach a number of average monthly active recipients of the service in the EU equal to or higher than 45 million and are designed as such by the European Commission (EC). In 2023 the EC designated 17 services as VLOPs (see Table 2 below). OSEs with the same reach shall be designated as **very large online search engines** (**VLOSEs**) and thus subject to the same obligations as VLOPs.[325] VLOPs and VLOSEs are particularly relevant given their impact on "facilitating public debate, economic transactions and the dissemination to the public of information, opinions and ideas and in influencing how recipients obtain and communicate information online".[326]

Table 2: Very large online platforms and search engines.
On April 2023, the EC designated 17 VLOPs and 2 VLOSEs:[327] ● VLOPs: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube and Zalando. ● VLOSEs: Bing, Google Search.
On December 2023, the EC designated 3 new VLOPs: Pornhub, Stripchat and XVideos.[328] During 2024, Shein[329] and Temu[330] were also designated as VLOPs.
It is interesting to note that only three from the total of 24 platforms are owned by EU-based companies (Dutch Booking.com, German Zalando, and Czech XVideos.com), while the rest are owned by companies based in the US, China and Canada.

1.2.1. Territorial scope

The regulation applies to digital services providers with establishment in the EU, same as the E-Commerce Directive.[331] However, the DSA innovates on this point and follows a similar formula to the GDPR, as it also has an extraterritorial reach, as its rules may apply to intermediaries without an establishment in the EU. The DSA requires a substantial connection to the EU,[332] which also occurs when

[324] Article 3(j) DSA.
[325] Article 33, DSA.
[326] Recital (75), DSA.
[327] DSA: Very Large Online Platforms and Search Engines (europa.eu)
[328] Commission designates second set of Very Large Online Platforms under the Digital Services Act | Shaping Europe's digital future (europa.eu)
[329] Commission designates Shein as Very Large Online Platform under the Digital Services Act | Shaping Europe's digital future (europa.eu)
[330] Commission designates Temu as Very Large Online Platform under the Digital Services Act | Shaping Europe's digital future (europa.eu)
[331] Article 2(1), DSA; Article 3(1), E-Commerce Directive.
[332] Recital (7), DSA.

the digital services are offered to a significant number of recipients in the EU or targeted towards their MS,[333] irrespective of where the providers of those intermediary services have their place of establishment.[334] That explains why several non-European providers have been labelled as VLOPs by the EC (see Table 2 above).

1.3. Main provisions

The obligations imposed on intermediary services providers by the DSA are built in a structure of cumulative obligations related to each category of providers.[335]

It is important to note that the DSA does not impose a general duty on intermediaries to monitor content or actively seek facts or circumstances indicating illegal activity.[336] This follows the rule of Article 15 of the E-Commerce Directive, which was also confirmed in several cases by the CJEU.[337]

The obligations established for each category of digital service providers are the following:

a) *Providers of intermediary services:*

- Cooperation with national (judicial and administrative) authorities following orders to act against illegal content or provide information.[338]
- Single points of contact for European and national authorities and users.[339]
- Legal representative for providers without an establishment in the EU.[340]
- Terms and conditions written in clear, plain, intelligible, user-friendly and unambiguous language, which must be publicly available in an easily accessible and machine-readable format.[341]
- Publication of transparency reports in a yearly basis.[342]

b) *OPs:*

- All obligations are mentioned in Section 3.1.
- Notice-and-action mechanisms and obligation to provide information to users affected by restrictions (extended to all 'hosting' services).[343]
- Notification of suspicions of criminal offences (extended to all 'hosting' services).[344]

---

[333] Article 3(e), DSA.
[334] Article 2(1), DSA.
[335] Cf. Turillazzi, A. et. al, 'The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications' (2023) 15 Law, Innovation and Technology 83, https://doi.org/10.1080/17579961.2023.2184136.
[336] Article 8, DSA.
[337] See: Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, ECLI:EU:C:2019:821; Case C-360/10, SABAM v Netlog, ECLI:EU:C:2012:85.
[338] Articles 9-10, DSA.
[339] Articles 11-12, DSA.
[340] Article 13, DSA.
[341] Article 14, DSA.
[342] Article 15, DSA.
[343] Articles 16-17, DSA.
[344] Article 18, DSA.

- Internal complaint-handling system against the decision taken by providers and out-of-court dispute settlement.[345]
- Trusted flaggers of illegal content.[346]
- Measures and protection against users providing manifestly illegal content.[347]
- Enhanced transparency reporting obligations (also for OSEs).[348]
- Prohibition of online interface design and organization that deceives or manipulates the recipients of their service.[349]
- Transparency of recommender systems and online advertisement.[350]
- Online protection of minors' privacy, safety, and security.[351]
- Additional obligations for online marketplaces ("KYBC", compliance by design, right to information).[352]

c) *VLOPs and VLOSEs:*

- All obligations mentioned in Sections 3.1. and 3.2.
- Risk assessment from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services,[353] and implement reasonable, proportionate and effective mitigation measures for the identified risks.[354]
- Crisis response cooperation when requested by the EC.[355]
- Enhanced transparency of recommender systems and online advertisement.[356]
- Data sharing with authorities and researchers.[357]
- Publication of transparency reports every six months.[358]
- Drafting of codes of conduct and crisis protocols when requested by the EC.[359]
- Independent audits conducted at their own expense and at least once a year, to assess compliance with their obligations and commitments undertaken pursuant to the codes of conduct and the crisis protocols.[360]
- Terms and conditions must be published in the official languages of all the MS in which they offer their services and include a concise, easily-accessible and machine-readable summary.[361]

[345] Article 20, DSA.
[346] Article 22, DSA.
[347] Article 23, DSA.
[348] Article 24, DSA.
[349] Article 25, DSA.
[350] Articles 26-27, DSA.
[351] Article 28, DSA.
[352] Articles 30-32, DSA.
[353] Article 34, DSA.
[354] Article 35, DSA.
[355] Article 36, DSA.
[356] Articles 38-39, DSA.
[357] Article 40, DSA.
[358] Article 42, DSA.
[359] Articles 45(1) and 48, DSA.
[360] Article 37, DSA.
[361] Article 14, DSA.

2. Applicability to XR

2.1. Subjects regulated within the XR ecosystem

From the simple analysis of the definitions given by Article 3 DSA, it appears that most XR services and applications fall into the scope of the DSA as intermediary services and also as OPs since they store and disseminate information to the public.

Regarding the specific category of VLOPs, some services using AR functionalities are subject to this regime by the decision of the EC (see Table 2 above): Google Maps, Instagram (social media) and Snapchat (instant messaging). However, in all these cases AR is not the main feature of the applications, but just a complement to their core function. In fact, no XR-focused service has been included in the first decision of VLOPs by the EC.

Taking into account the threshold of 45 million average monthly active users in the EU, it is very unlikely that new XR-focused platforms, especially those providing VR solutions, will be added to VLOPs regime in the short term. Some of the most known 'metaverse' platforms are far from this amount, including Horizon Worlds by Meta, which by the end of 2022 had only 200,000 active users world-wide.[362] This comes as little surprise, given that this industry is still developing and there are some barriers to massive adaptation (e.g., high cost of VR headsets).[363]

Some videogames that use virtual worlds (although they cannot be strictly described as XR applications) might reach the number of monthly users.[364] Roblox, with its estimated 30.9 million monthly active users in the EU (as of February 2024), is a significant player. As it continues to grow, potentially exceeding 45 million monthly active users, it could be designated as a VLOP in the coming months.[365]

2.2. Obligations for XR providers

Providers of social media and other applications using AR, VR platforms, online virtual worlds, and other XR solutions are likely to be subject to the obligations for OPs under the DSA, even provided they have a substantial connection with the EU. The implementation of these obligations to the diverse services inherent to the XR industry needs thoughtful consideration.

Obligations related to handling and tackling of illegal content are especially relevant for XR providers, given that the immersive characteristics of the technology can enhance its harmful effects on users. One particular challenge in this context is disinformation, which could be considered illegal under the legislation of certain MS, but also as socially harmful content, which has to be identified through risk assessment by VLOPs and VLOSEs.[366] XR providers may also subscribe codes of conduct under request of the EC, as it has been done in matter of disinformation with the 2022 Code of Practice on Disinformation, which is expected to be recognised as a code of conduct under the DSA.[367]

[362] Hey Fellow Kids: Meta Is Revamping Horizon Worlds to Attract More Teen Users (gizmodo.com)
[363] XR4Human, Policy Report, p. 30.
[364] Metaverse Monthly Users Worldwide - Market size in metaverse? (metaverseofthing.com)
[365] EU Digital Services Act – Roblox Support
[366] Chambers and Partners, The Digital Services Act (DSA) and combating disinformation – 10 key takeaways
[367] The 2022 Code of Practice on Disinformation (europa.eu)

Some obligations that are innovations of the DSA may have uttermost importance in the XR context. For example, the prohibition for providers of OPs to design and organise the online interface in a way that deceives or manipulates users,[368] which is commonly known as "dark" or "deceptive patterns". Deceptive patterns, as emotional persuasion and predatory monetisation have been identified in some virtual games,[369] and they may be particularly harmful in XR environments, considering the high emotional investment showed by certain users in these platforms.[370] The prohibition on deceptive patterns was not part of the original DSA proposal issued by the EC, but emerged during the negotiations with the European Parliament. The argument was that transparency obligations may be ineffective in tackling these practices and that only the imposition of a general ban on these practices, similar to the prohibition of 'unfair commercial practices' in the Unfair Commercial Practices Directive (UCPD), may be more effective.[371] It is important to stress that the prohibition just refers to deceptive patterns embedded in the design or organisation of the OP's interface, therefore other deceptive practices may be out of the scope of the DSA (but eventually covered by another legislation, e.g., the UCPD).

Another important obligation is the implementation of appropriate and proportionate measures to protect minors' privacy, safety, and security.[372] One of the main conclusions of our policy report was that XR technologies can be incredibly impactful on children,[373] and the measures to control the exposure of children to harmful contents in XR platforms (i.e. the age verification mechanisms) appear to be weak.[374] However, this rule must be backed up by adequate supervision by the authorities, otherwise it may be no more than a declaration of intent.

However, the DSA is not built on a risk-based approach, relying only on the criteria of services functionalities and user amount when it comes to establishing the different sets of cumulative responsibilities. Risk assessment only appears as a specific obligation for services designed as VLOPs but is not mandatory for the rest of OPs. The main effect is that most XR platforms will have reduced or softened obligations than regular social media platforms, given that they do not reach 45 million EU users. For example, an OP such as Horizon Worlds is not forced to conduct risk assessments, or to report on the ways they do advertisement. In our opinion this is contradictory, given that XR platforms pose increased risk of harming users by the technologies involved, which are immersive by definition.

[368] Article 25, DSA.
[369] [Investigating Players' Perceptions of Deceptive Design Practices within a 3D Gameplay Context | Proceedings of the ACM on Human-Computer Interaction]
[370] XR4Human, Policy Report, p. 39.
[371] https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en, pp. 7, 81.
[372] Article 28, DSA.
[373] XR4Human, Policy Report, pp. 38-39.
[374] Here's what it's like inside Meta's virtual world | CNN Business

6.3. Digital Markets Act

1. Overview of the regulation

1.1. Scope

The Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector or **Digital Markets Act** (**DMA**) is an EU regulation that aims to ensure a level playing field for the markets in the digital sector in general, and for users of large online companies in particular.[375] The DMA was published in the Official Journal of the EU on 10 October 2022 and enacted 1 November 2022. It is fully applicable from 2 May 2023.

The DMA establish the conditions for large online providers to be recognised as 'gatekeepers' by the Commission, gives them specific obligations and prohibitions, and empowers the EC to enforce the regulation and impose remedies.[376]

1.2. Subjects

Under the DMA, companies may be recognised as **gatekeepers** provided that they meet a list of cumulative qualitative criteria, which is presumed to be satisfied (and thus forces companies to disclose this information to the EC) when the company meets the related quantitative criteria.[377]

Table 3: Gatekeeper's criteria

Qualitative criteria[378]	**Quantitative criteria**[379]
i. To have a significant impact on the internal market	the company achieves an annual EU turnover equal to or above EUR 7,5 billion in each of the last three financial years, or its average market capitalisation amounted to at least EUR 75 billion in the last financial year, and it provides a core platform service in at least three EU MS.
ii. To provide a '**core platform service**' (CPS) which is an important gateway for business users to reach end users.	The CPS has at least 45 million monthly active EU end users service in the last financial year and at least 10,000 yearly active EU-based business users.
iii. To enjoy an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.	The quantitative criteria in number ii. was met by the CPS in each of the last three financial years.

The types of CPS provided by the gatekeepers are the following:[380]

375

376 About DMA (europa.eu)

377 The difficulty of designating gatekeepers under the EU Digital Markets Act (bruegel.org)

378 Article 3(1), DMA

379 Article 3(2), DMA

380 Article 2(1), DMA

(a) online intermediation services (OIS),
(b) online search engines,
(c) online social networking services,
(d) video sharing platform services,
(e) messaging services (N-IICS),
(f) operating systems,
(g) web browsers,
(h) virtual assistants,
(i) cloud computing services, and
(j) online advertising services.

In September 2023, six companies were designated by the EC as gatekeepers, providing a total of 22 CPSs. One gatekeeper and two 2 CPP have been designated during 2024. These are the following:[381]

Table 4: Current gatekeepers and CPSs (as April 2024)

Gatekeepers	Core platform services	Type
Alphabet (8 CPSs)	Google Maps, Google Play, Google Shopping	OIS
	Google	Advertising
	Android	Operating system
	Google Search	Search engine
	YouTube	Video sharing
	Chrome	Browser
Amazon (2 CPSs)	Amazon Marketplace	OIS
	Amazon	Advertising
Apple (4 CPSs)	App Store	OIS
	iOS	Operating system
	Safari	Browser
	iPadOS	Operating system
ByteDance (1 CPS)	TikTok	Social network
Meta (6 CPSs)	Facebook, Instagram	Social network
	Meta Marketplace	OIS
	WhatsApp, Messenger	Messaging (N-IICS)
	Meta	Advertising
Microsoft (2 CPSs)	LinkedIn	Social network
	Windows PC OS	Operating system
Booking (1 CPS)	Booking.com	OIS

Gatekeepers have six months from their designation to comply with the provisions of the DMA, so the first designated companies had to comply with their obligations by 6 March 2024.

[381] DMA designated Gatekeepers (europa.eu)

1.3. Territorial scope

As the definition of gatekeepers is based on the number of EU-based users and financial records, the law does not require gatekeepers to have an establishment in the EU. This extraterritorial reach is explicit the DMA, by saying the regulation applies "irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service"[382]. In fact, just one gatekeeper (Booking) of a total of seven has its main establishment in the EU (see Table 4 above).

1.4. Main provisions

The DMA imposes obligations on gatekeepers and prohibits certain practices, including the following:

(a) Data merging and reuse: Unless given consent by the user under the terms of the GDPR, the gatekeeper shall not do any of the following:[383]

- process, to provide online advertising services, personal data of end users using services of third parties that make use of CPS of the gatekeeper;
- combine personal data from the relevant CPS with personal data from any further CPS or from any other services provided by the gatekeeper or with personal data from third-party services;
- cross-use personal data from the relevant CPS in other services provided separately by the gatekeeper, including other CPS, and vice versa; and
- Sign in end users to other gatekeeper services in order to combine personal data.

(b) Vendor lock-in: The gatekeeper shall not prevent business users from offering the same products or services to end users through third-party OIS or through their own direct online sales channel at prices or conditions that are different from those offered through the OIS of the gatekeeper.[384]

(c) Business-user interaction: The gatekeeper shall allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its CPS or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the CPS of the gatekeeper.[385] The gatekeeper shall allow end users to access and use, through its CPS, content, subscriptions, features or other items, by using the software application of a business user, including where those end users acquired such items from the relevant business user without using the CPS of the gatekeeper.[386]

(d) Bundling: The gatekeeper shall not require end or business users to use, to offer, or to interoperate with, an identification service, a web browser engine or a payment service, or technical services that support the provision of payment services (e.g. payment systems for in-app purchases) of that gatekeeper in the context of services provided by the business users using that gatekeeper's CPS.[387]

(e) Un-installability: The gatekeeper shall allow and technically enable end users to easily un-install any software applications on the operating system of the gatekeeper, without prejudice to the

[382] Article 1(2), DMA
[383] Article 5(2), DMA
[384] Article 5(3), DMA
[385] Article 5(4), DMA
[386] Article 5(5), DMA
[387] Article 5(7), DMA

possibility for that gatekeeper to restrict such un-installation in relation to software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third parties.[388]

(f) Device neutrality: The gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant CPS of that gatekeeper.[389]

(g) Self-preferencing: The gatekeeper shall not treat more favourably, in ranking and related indexing and crawling, services and products offered by the gatekeeper itself than similar services or products of a third party. The gatekeeper shall apply transparent, fair and non-discriminatory conditions to such ranking.[390]

(h) Interoperability: The gatekeeper shall allow providers of services and providers of hardware, free of charge, effective interoperability[391] with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via their operating system or virtual assistant as are available to services or hardware provided by the gatekeeper.[392]

(i) Data portability: The gatekeeper shall provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant CPS, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data.[393]

2. Applicability to XR

2.1. Subjects regulated within the XR ecosystem

The DMA does not regulate specific technologies, but companies, provided they meet the criteria to be designated as gatekeepers (see Table 3 above). Regarding the XR ecosystem, several types of CPS are related to XR and thus might be regulated by the DMA:

(a) Online social networking service: means a platform that enables end users to connect and communicate with each other, share content and discover other users and content across multiple devices and, in particular, via chats, posts, videos and recommendations.[394] This definition may apply to the so-called 'metaverse(s)' or other virtual environments that allow the interaction of users (e.g. VR games, virtual meeting rooms).

(b) Virtual assistant: means a software that can process demands, tasks or questions, including those based on audio, visual, written input, gestures or motions, and that, based on those

[388] Article 6(3), DMA
[389] Article 6(4), DMA
[390] Article 6(5), DMA
[391] Interoperability is defined as "the ability to exchange information and mutually use the information which has been exchanged through interfaces or other solutions, so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function" (Article 2(29), DMA).
[392] Article 6(7), DMA
[393] Article 6(9), DMA
[394] Article 2(7), DMA

demands, tasks or questions, provides access to other services or controls connected physical devices.[395] This definition includes virtual assistants that are deployed through XR hardware (e.g. remote assistants that are used in manufacturing)[396].

(c) Online advertising services: the DMA establishes that this concept covers any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the other CPS. Therefore, if advertisement is deployed on an XR CPS, then this would be also considered as a CPS.

(d) Online intermediation services (OIS): In general, XR services that are not covered by other examples may be covered by OIS, which are defined by Regulation 2019/1150[397] as those services which meet all of the following requirements:[398]

- they constitute information society services, which are "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[399]
- they allow business users to offer goods or services to consumers with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded.
- they are provided to business users based on contractual relationships between the provider of those services and business users who offer goods or services to consumers.

2.2. Obligations for XR providers

There are several obligations of the DMA that will be relevant to the gatekeepers within the XR ecosystem.

Firstly, the obligations restricting the **sharing of data** among the gatekeeper's services, unless end-users provide their consent, which has to be freely given, specific, informed and unambiguous.[400] Even if the XR application has not been designated as CPS, the DMA states that gatekeepers are limited when combining or cross-using personal data from one of their CPS with other services provided by the gatekeeper. Meta, for example, may not share Facebook data with Virtual Worlds, except when consented by its end-users. This limits the ability of companies to use other legal bases (contained in Article 6 GPDR) for data sharing between their own services. Bases such as performance of contract or legitimate interest are usually described in the privacy policy or terms and conditions of services that most end users do not read, so this provision avoids that. The obligation of requesting consent also means that individuals can withdraw it at any time, so companies need to provide the means to revoke permission for such sharing.

Secondly, another obligation that is of special relevance for the XR ecosystem is **device neutrality**, that forces gatekeepers to allow the use of third-party services or apps stores in their devices and not restrict them to their own CPS. This means that manufacturers of XR devices may not restrict sideloading or alternate app stores in headsets. For example, Apple had to make an historical change and open these

[395] Article 2(12), DMA
[396] XR4Human, Policy Report, p. 17.
[397] Article 2(5), DMA
[398] Article 2(2), Regulation (EU) 2019/1150
[399] Article 1(1)(b), Directive (EU) 2015/1535
[400] See GDPR section.

practices for EU-based users of iPhone and iPad.[401] However, the company might avoid this obligation on their XR products as its launching a new operating system and app store for the Vision Pro headset,[402] which will not be classified as CPS (like iOS and the App Store) until Apple Vision reach the user thresholds of the DMA.

Thirdly, gatekeepers obligations on **interoperability** may allow third party software or hardware XR providers to effectively integrate or connect with CPS, free of charge. The implementation of this obligation, however, may require the development of technical standards by European standardisation bodies by request of the EC.[403]

A similar effect will have the **provisions on preferential treatment** of the gatekeeper's own services over third-party on their apps stores, given that some of the most important XR hardware providers are part of a holding has also runs social media or other online platforms. For example, Google must not forcedly rank first YouTube on their VR store when customers search for a video streaming service.

2.3. Challenges

The main challenge for the applicability of the DMA to the XR ecosystem is that not many XR companies and services meet the criteria to be designated as gatekeepers and CPSs, respectively. This is a consequence of the reduced reach of XR hardware in the European consumers, as previously analysed.[404]

(a) Impact on the internal market: The qualitative criteria to presume this impact does not look at the services in particular but at the companies as a whole. Big tech players offering XR solutions and functionality already meet this criterion as identified by the EC, including Meta (AR and VR), ByteDance (AR), Google (AR and VR), Microsoft (VR) and Apple (VR).[405]

(b) Provide a CPS: Even when some services incorporating AR functionalities (e.g., TikTok, Instagram, Google Maps) or app stores selling XR applications (Google Play, Apple's App Store) have already been designated as CPS, the current state of the XR industry leaves little room for new VR services (including 'metaverses') to meet the thresholds for being recognised as CPS.

(c) Enjoy an entrenched and durable position: The difficulty for XR services to meet the criteria of number ii. means that they would not meet this criterion either.

This challenge is exacerbated by the fact that gatekeepers may create new services for the XR environment to avoid using their services already designated as CPS (such as operating systems and application stores), as could happen in the case of Apple Vision Pro.

401 Apple is bringing sideloading and alternate app stores to the iPhone - The Verge
402 Apple Vision Pro - Apple
403 Recital 96, DMA
404 See DSA section.
405 See Table 4 above.

7. Cybersecurity

7.1. Convention on Cybercrime

1. Overview

1.1 Scope

The Convention on Cybercrime was adopted in Budapest in 2001 by the CoE and entered into force in July 2004. As each MS in the EU is a member of the CoE, the provisions of the Convention of Cybercrime are applicable to each MS. The Convention on Cybercrime is particularly necessary because the Internet creates new affordances in crime, i.e., cybercrimes. This cross-border nature of crimes presents novel challenges in terms of overlapping jurisdiction, new forms of crimes, and international cooperation between countries for coordinated criminal investigations. The Convention of Cybercrime aims to create a multilateral international law instrument on cybercrime. It sets out provisions on substantive and procedural cybercriminal law, jurisdiction and international cooperation. As criminal law is, with some exceptions, outside the purview of regional legislation, this multilateral framework ensures cooperation between signatories, and sets out procedures to tackle the nature of cross-border cybercrimes is necessary for parties.[406]

1.2 Subjects

The Convention on Cybercrime has been signed by seventy-two parties, and its provisions are applicable to all its signatories.[407] This includes all members of the CoE (which include all MS of the EU), as well as other signatories from across all continents globally. However, not all countries have ratified each of their obligations under the Convention on Cybercrime. For example, Ireland has currently ratified the substantive cybercrime provisions of the Convention on Cybercrime through the Criminal Justice (Offences Relating to Information Systems) Act 2017, while ratifying the full suite of procedural powers under the Convention on Cybercrime is currently underway.[408] Similarly, the current domestic laws in Sweden correspond with several of the substantive and procedural obligations under the Convention on Cybercrime, but full ratification is still pending.[409]

However, the Convention on Cybercrime sets out some obligations for parties that have a direct bearing on private entities. For this, the Convention on Cybercrime defines computer systems and service providers. Computer systems are broadly defined, and include devices that automatically process data, which covers XR headsets and handsets in its ambit. Similarly, service providers include private entities that either enable users to communicate through a computer system or process/store computer data relating to such communication services, which would also cover providers of XR-based services that allow communication.

[406] Jentley Lenong '*State Cybersecurity Governance in the Fourth Industrial Revolution: An International Law Perspective*' in Wesley Doorswamy, Babu Sena Paul, Tshilidzi Marwala (eds.) The Disruptive Fourth Industrial Revolution (Lecture Notes in Electrical Engineering 674, Springer 2020) p. 84-85.
[407] 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY' Council of Europe <https://www.coe.int/en/web/cybercrime/parties-observers>
[408] Octopus Cybercrime Community 'Cybercrime Legislation- Ireland' Council of Europe <https://www.coe.int/en/web/octopus/-/ireland>
[409] Ibid.

1.3 Main provisions

The obligations under the Convention on Cybercrime can be broadly classified under four heads:

(a) Substantive cybercrime provisions: The Convention on Cybercrime requires all Parties to set out certain cybercrimes as criminal offences in their respective domestic laws. The purpose of these provisions is to harmonise the understanding illegal behaviour online and create standards of 'dual criminality'. Harmonising criminal offences across borders seeks to ensure that illegal behaviour in Country A is also illegal in Country B, increasing the ease through which cross-border law enforcement investigations can be carried out. This includes:

  i. Offences against the confidentiality, integrity and availability of computer data and computer systems: The Convention on Cybercrime requires Parties to criminalise illegally accessing computer systems, illegally intercepting computer data, interfering with the integrity of computer data, interfering with the functioning of a computer system, and to produce, procure, transmit or otherwise make available any device available that can be used for the committing the above offences.[410] These provisions largely protect against hacking, altering data, creating or distributing malware, or otherwise negatively impacting the core security aspects of a computer system or computer data.

  ii. Computer related offences: The Convention on Cybercrime requires Parties to criminalize illegally engaging in computer-related forgery, i.e., inputting, altering, deleting or suppressing computer data resulting in inauthentic data with the intention that the inauthentic data is considered as authentic data.[411] It also requires Parties to similarly criminalize computer-related fraud, where interfering with the integrity of the computer data or the computer system causes a loss of property to an individual, and is conducted with a fraudulent or dishonest intent to create an economic benefit for the perpetrator.[412]

  iii. Content- related offences: The Convention on Cybercrime requires Parties to criminalize offences relating to child pornography. This provision is broadly worded, including producing, offering, transmitting, procuring or possessing child pornography on or through a computer system.[413] The Convention on Cybercrime defines 'child pornography' as any pornographic material that visually depicts minors, persons appearing to be minors, or realistic images representing minors which are engaged in sexually explicit conduct.[414] The Convention on Cybercrime also requires Parties to criminalize the intentional infringement of copyright on a commercial scale through computer systems.[415]

(b) Procedural cybercrime provisions: The Convention on Cybercrime requires all Parties to ensure that their domestic laws contain certain procedural provisions necessary for investigating cybercrimes. These powers and procedures in domestic law must be subject to

[410] Art. 2-6, Convention on Cybercrime.
[411] Art. 7, Convention on Cybercrime.
[412] Art. 8, Convention on Cybercrime.
[413] Art. 9(1), Convention on Cybercrime.
[414] Art. 9(2), Convention on Cybercrime.
[415] Art. 10, Convention on Cybercrime.

Funded by the European Union

safeguards in domestic law that protect human rights and liberties consistent with international standards such as the CoE's European Convention for the protection of Human Rights and Fundamental Freedoms, 1950 and the UN's Fundamental Freedoms and the International Covenant on Civil and Political Rights, 1966.[416] These procedural provisions include measures that enable the competent authorities to:

i. Obtain expeditious preservation of stored computer data by obliging the person possessing or controlling the computer system to preserve and maintain the integrity of that data for a maximum of 90 days. [417] This provision is relevant where the computer data is otherwise particularly prone to loss or modification;

ii. Preserve and obtain partial disclosure of traffic data to enable the competent authorities to identify the service providers transmitting the communication and the path through which the communication was transmitted[418];

iii. Require service providers to collect or record real-time traffic data associated with specified communications through technical means by themselves or assist the competent authorities in this process[419]; and

iv. Require service providers to collect or record real-time content data of specified communications through technical means by themselves or assist the competent authorities in this process[420];

(c) Jurisdiction: The Convention on Cybercrime requires Parties to adopt legislative measures that establish their jurisdiction over the aforementioned cybercrimes. This would enable a party to assume jurisdiction when the specific offence is committed in (1) its territory (including on board a ship flying the flag of that party or an aircraft registered under the laws of that party) or (2) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the jurisdiction of other states. Importantly, the Convention on Cybercrime clarifies that it does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.[421] This enables Parties to create laws that can include actors or actions committed outside its own jurisdiction, if the effects of that action are felt in that State. The Convention on Cybercrime clarifies that in instances where multiple Parties claim jurisdiction over an offence, the involved Parties must consult each other and devise the appropriate jurisdiction for prosecution. [422]

(d) International cooperation: The Convention on Cybercrime obliges Parties to afford mutual assistance to each other for the purposes of investigations or proceedings relating to cybercrimes, through either the provisions of the law in the requested Party or through treaties on mutual legal assistance.[423] In the absence of any mutual assistance treaties, the Convention on Cybercrime sets out a framework through which assistance can be requested and treated between Parties, including the designation of central authorities responsible for

[416] Art. 15, Convention on Cybercrime.
[417] Art. 16(1), Convention on Cybercrime.
[418] Art. 17, Convention on Cybercrime.
[419] Art. 20, Convention on Cybercrime.
[420] Art. 21, Convention on Cybercrime.
[421] Art. 22(4), Convention on Cybercrime.
[422] Art. 22(5), Convention on Cybercrime.
[423] Art. 25, Convention on Cybercrime.

sending or receiving requests for mutual assistance.[424] The Convention on Cybercrime sets out specific provisions for requests relating to preserving traffic data or stored computer data, requests to accessing stored computer data, requests for real-time collection of traffic data and requests for interception of traffic data.[425] The Convention on Cybercrime also requires each Party to designate a point of contact available on a 24/7 basis to provide immediate assistance for investigations or proceedings relating to cybercrimes or to collect electronic evidence for criminal offences.[426]

2. Applicability to XR technology

2.1 Subjects regulated within the XR ecosystem

At the outset, the provisions of the Convention of Cybercrime apply only to the Parties at the national level and are not directly applicable to entities in the XR ecosystem. However, Parties are required to adopt the provisions in the Convention on Cybercrime in their national criminal laws, which might be relevant for users, developers, and service providers in the XR ecosystems. As discussed in Section 1.2 above, service providers might be required to comply with directions issued pursuant to domestic legal provisions mandated by the Convention on Cybercrime.

2.2 Obligations for XR providers

The primary obligations for XR service providers would be based on domestic criminal laws, particularly in terms of cooperating with the competent authorities in investigations or proceedings concerning criminal offences. This would include the obligations to (a) preserve traffic data, (b) to assist in collecting or recording traffic data in real time or intercept content data in real time for specified communications, and (c) disclose the preserved traffic data.[427] A Party to the Convention on Cybercrime may also issue a production order, requiring service providers to submit subscriber information relating to its services in their possession or control.[428] The EU has adopted Regulation 2023/1543 on European Production Orders and European Preservation Orders, which shall be applicable from 18 August 2026.[429] This is expected to reduce the time taken between authorities of signatory countries in sharing electronic evidence for cybercrimes.

Additionally, the substantive cybercrime provisions are relevant for XR providers, as the XR ecosystem is susceptible to the cybercrimes covered by the Convention, such as hacking, forgery, fraud, malware, and child pornography. However, the Convention on Cybercrimes is silent on newer forms of cybercrimes that are unique to the XR ecosystem, such as virtual identity theft and virtual rape. This report notes the unique concerns with virtual sexual assaults in analysing the CSAR.[430] WP 2.1 notes the potential of virtual identity theft through hacking. The Convention of Cybercrime does require Parties to criminalise illegal

[424] Art. 27, Convention on Cybercrime.
[425] Art. 30-34, Convention on Cybercrime.
[426] Art. 35, Convention on Cybercrime.
[427] Arts. 17(1), 20(1)(b), 30, Convention on Cybercrime.
[428] Art. 18(1)(b), Convention on Cybercrime.
[429] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, p. 118–180.
[430] See CSAR section.

access, computer forgeries and computer frauds, which specifically address various aspects of virtual identity theft.

Lastly, the Convention on Cybercrime provides a framework for international cooperation through mutual assistance between Parties. However, it does not clarify the question of jurisdiction, leaving that to the Parties to mutually discuss and agree upon. These nuances need to be closely considered when analysing the impact of the Convention of Cybercrimes on the XR ecosystem.

Funded by the European Union

7.2. Network and Information Security Directive

1. Overview

1.1 Scope

The Directive 2002/2555 ("**NIS2 Directive**") replaces the Directive 2016/1148, i.e., the "NIS Directive" in aiming to ensure a high level of cybersecurity across the EU. The previous NIS Directive was replaced to reduce the disparities in the internal market due to cybersecurity requirements imposed by various MS. These disparities were likely to cause a higher vulnerability to security incidents, which would also have caused significant damage to the cross-border nature of the internal market of the EU. For these reasons, the NIS2 Directive was enacted, keeping in mind the need to harmonize and update obligations towards cybersecurity applicable to both MS and towards the entities covered within the scope of this directive.

1.2 Subjects

The NIS2 Directive imposes obligations directly on the MS, regarding institutional measures and mechanisms to be adopted, and cooperation on cybersecurity incidents and threats within the EU. Additionally, the NIS2 Directive also imposes certain obligations on private network and information system (**NIS**) entities, which shall be the focus of discussion within this section. The NIS 2 Directive flags the key sectors which are of importance for the functioning of MS or the internal market of the EU. These are set out as two Annexes to the NIS2 Directive, which also detail the type of entities typically covered within the sector (aka "**Covered Entities**").

Annex I refers to entities operating in 'sectors of high criticality', i.e., energy, transportation, banking, health, financial market infrastructures, digital infrastructures and ICT service management sectors. Here, digital infrastructures would refer to the basic building blocks of the digital sector, including the Internet Exchange Point providers, DNS service providers (other than root name servers), top level domain (TLD) name registries, data centre service providers, content delivery service providers etc.[431] Similarly, Annex II refers to entities operating in 'other critical sectors', which includes, *inter alia*, postal services, waste management, manufacturing, and digital providers. Digital providers here refer to providers of online marketplaces, search engines and social media services.[432]

The NIS2 Directive applies to all NIS entities in the above sectors operating within the EU that (a) employ more than 50 persons, (b) have an annual turnover greater than EUR 10 million, and (c) have a balance sheet total above EUR 10 million can be classified as medium sized enterprises.[433] Similarly, the NIS2 Directive applies to the above entities even if they do not reach the foregoing medium-sized enterprise threshold if they are critical to the MS or play a significant and systemic role in societal or economic activities.[434] The NIS2 Directive also applies to NIS entities identified as critical entities under the Directive 2022/2557[435].

[431] Para 8, Annex I, NIS2 Directive.
[432] Para 6, Annex II, NIS2 Directive.
[433] Art. 2 of the Annex to Recommendation 2003/361/EC.
[434] See Art. 2 for the complete description of NIS entities covered by the NIS2 Directive.
[435] This refers to entities identified by 17 July 2026 by each member state as critical entities for the sectors listed in the Annex to Directive 2022/2557. The sectors are broadly similar to Annex I of the NIS2

Funded by the European Union

The NIS2 Directive thus applies, in varying ways to the Covered Entities, since the NIS2 Directive divides them into essential entities and important entities. Under the NIS2 Directive, **Essential Entities** include[436]:

i. entities falling within Annex I (sectors of high criticality) that exceed the threshold of medium-sized enterprises;
ii. qualified trust service providers, TLD name registries and DNS service providers regardless of their size;
iii. providers of electronic communication services and electronic communication networks that qualify as medium-sized enterprises;
iv. public administration entities within the ambit of the NIS2 Directive;
v. any other entity of a type referred to in Annex I or Annex II identified by a MS as essential entities;
vi. entities identified as critical entities under Directive 2022/2557;
vii. entities identified by MS as operators of essential services in accordance with Directive 2016/1148.

All other entities operating in the sectors referred to in Annex I or II which do not qualify as essential entities shall be considered as **Important Entities**, including all Covered Entities which have been identified by a MS as important entities.[437] Regarding this distinction, it is helpful to note that Essential Entities and Important Entities are treated mainly equally. However, the NIS2 Directive prescribes additional supervisory and enforcement powers over Essential Entities and imposes higher penalties for failing to comply with their obligations under this law.[438]

1.3 Main provisions

(a) Obligations on MS and EU bodies: The NIS2 Directive imposes several obligations on each MS in terms of adopting a national cybersecurity strategy[439], establishing competent authorities[440], designing a national cyber-crisis management framework to respond to large-scale cybersecurity incidents[441], establishing a computer security incident response team (CSIRT) which shall monitor, detect, respond, and assist in handling cyber threats, vulnerabilities, and incidents[442]. It requires cooperation at the EU level through the role of a Cooperation Group[443], the CSIRT network between MS[444] and the European cyber crisis liaison organisation network[445].

(b) Obligations impacting Covered Entities:

Directive, with minor changes such as the omission of ICT service management (B2B) and the inclusion of production, processing and distribution of food, and the inclusion of public transport in the transport sector.

[436] Art. 3(1), NIS2 Directive
[437] Art. 3(2), NIS2 Directive.
[438] Art. 32, NIS2 Directive.
[439] Art. 7, NIS2 Directive.
[440] Art. 8, NIS2 Directive.
[441] Art. 9, NIS2 Directive.
[442] Art. 10(1) read with Art. 11(3), NIS2 Directive.
[443] Art. 14, NIS2 Directive.
[444] Art. 15, NIS2 Directive.
[445] Art. 16, NIS2 Directive.

i. MS must ensure that Covered Entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of their NIS used by these entities for their operations or providing their services. These measures must ensure a level of security appropriate to the risks posed to the NIS, considering the state-of-the-art, the costs involved and relevant European or international standards;

ii. The foregoing measures must include at least the following[446]:
   - policies on risk analysis and information system security;
   - incident handling;
   - business continuity, such as backup management and disaster recovery, and crisis management;
   - supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
   - security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure;
   - policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
   - basic cyber hygiene practices and cybersecurity training;
   - policies and procedures regarding the use of cryptography and, where appropriate, encryption;
   - human resources security, access control policies and asset management;
   - the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

(c) While undertaking these measures, and particularly the measures of ensuring supply chain security, the Covered Entities must consider the vulnerabilities specific to each direct supplier and service provider, their overall quality of products and their cybersecurity practices, thus focusing on the vulnerabilities in its upstream and downstream supply chain.[447]

(d) Covered Entities must notify the competent authority of any significant incident.[448] This involves submitting information at various stages, including submitting an early warning within 24 hours of becoming aware of the significant incident, an incident notification within 72 hours , and a final report within 1 month of submitting the incident notification giving a detailed description of the incident including its severity and impact, the threat or cause triggering the incident, the applied and ongoing mitigation measures, and the cross-border impact of the incident if any.

(e) Covered Entities must also inform the recipients of their services that are potentially affected by a significant cyber threat of the cyber threat itself as well as the measures or remedies that can be taken by the recipients.[449]

(f) MS may require Covered Entities to use ICT products, services and processes that are certified under European cybersecurity certification schemes adopted under Regulation 2019/881, i.e., the Cybersecurity Act.[450]

[446] Art. 21(2), NIS2 Directive.
[447] Art. 21(3), NIS2 Directive.
[448] An incident refers to an event that compromises the availability, authenticity, integrity or confidentiality of the data processed or services offered or accessible through network and information systems, see Art. 6(6), NIS2 Directive. An incident becomes a significant incident when it may cause severe operational disruption or financial loss of the entity, or if it may affect other natural or legal persons by causing them considerable material or non-material harm, see Art. 23(3), NIS2 Directive.
[449] Art. 23(2), NIS2 Directive.
[450] Art. 24, NIS2 Directive.

(g) Annex I entities which fall within the digital infrastructure and ICT service management sectors, as well as Annex II entities classified as digital providers (providers of online marketplaces, online search engines or social networking services platforms) ("**Covered Digital Entities"**) must designate a representative located in one of the MS where the services are being offered, if that entity is not established in the EU but offers services within the EU.[451] The Covered Digital Entities are required to submit information to the competent authority by 17 January 2025, to enable ENISA to create and maintain a registry of the Covered Digital Entities.[452]

1.4 Interaction with the Directive on Critical Entities Resilience

The Directive 2022/2557 on Critical Entities Resilience (**CER Directive**) aims to enhance the resilience of critical entities, and to protect and safeguard critical entities from all kinds of risks, including physical or cybersecurity risks, in the EU.[453] The CER Directive is designed to be implemented in a coordinated manner with the NIS2 Directive.[454] The CER Directive sets out broad obligations on risk assessment, resilience measures, background checks and incident reporting for identified critical entities.[455] This report does not discuss the CER Directive in further detail as the CER Directive specifically excludes the application of its obligations to the Covered Digital Entities under the NIS2 Directive.[456]

2. Applicability to XR

2.1 Subjects regulated within the XR ecosystem

The NIS2 Directive primarily focuses on bolstering the cybersecurity capabilities of the Covered Entities, and as such, is relevant to the XR ecosystem in both directly and indirectly. As with several other digital services, XR technologies, particularly the delivery of XR-based services, rely on other components of the larger digital infrastructure. Cybersecurity is particularly relevant for XR technologies due to the extent of processing of personal data and special categories of data, including biometric data. The NIS2 Directive's role in ensuring more significant cyber-security across the supply-chain, mainly keeping in mind the extent of personal data processing in XR technologies, has been highlighted in recent reports and studies.[457] However, the NIS2 Directive does not deal with cybersecurity requirements for XR devices (XR headsets and handsets) which are considered as consumer products.[458]

(a) *General Application of the NIS2 Directive to Covered Entities*: Once a NIS entity is considered a Covered Entity under the NIS2 Directive, it must adhere to its obligations under the NIS2 Directive. This can be true for any of the entities within the specified sectors, such as banking, healthcare, transportation or manufacturing. Accordingly, if any of these entities

---

[451] Art. 26(3), NIS2 Directive.
[452] Art. 27(2), NIS2 Directive.
[453] Art. 1, CER Directive.
[454] Art. 1(2), CER Directive.
[455] Arts. 12-15, CER Directive.
[456] Art. 8, CER Directive.
[457] Niels Vandezande 'Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor' (April 2024) Computer Law and Security Review 52 <https://www.sciencedirect.com/science/article/pii/S0267364923001000>
[458] Tambiama Madiega et al 'Metaverse Opportunities, risks and policy implications' (2022) Briefing PE 733.557, European Parliamentary Research Service < https://www.europarl.europa.eu/cmsdata/268589/eprs-briefing-metaverse_EN.pdf >

incorporates or integrates the use of XR-based functionalities within their operations, these Covered Entities, regardless of sector, might have to consider the cybersecurity risks posed by those XR-based functions. For example, if XR-based treatment or diagnostic methodologies are used by healthcare providers working within a Covered Entity, that Covered Entity may have to undertake the technical, organisational and operational cybersecurity measures and vet the supply chain for the XR services being used as part of their compliance with the NIS2 Directive.

(b) *Specific application of the NIS2 Directive to XR service providers*: The NIS2 Directive can also apply directly to entities providing XR-based services, in certain circumstances. The Covered Digital Entities under the NIS2 Directive includes a reference to digital infrastructure entities and digital provider entities. At this stage, no digital infrastructure services are provided through XR technology. Annex II includes providers of online marketplaces, online search engines, and online social networking services. The NIS2 Directive defines online marketplaces as '*a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers*'.[459] We note that current XR-based services in the market include both online marketplaces and online social networking services. For example, Amazon Web Services has partnered with Hexa 3D Commerce, an AR-based e-commerce entity and Obsess, a VR-based virtual store- both of which aim to be the next generation of retail e-commerce by providing a virtual and immersive shopping experience to users.[460]

Similarly, the NIS2 Directive defines 'social networking services platforms' as '*platforms that enable end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations*'.[461] This is a very wide-ranging definition that may even include any platform that allows end-users to communicate with each other even when the communication is a secondary functionality of the platform. There are several new XR-based entities offering social networking services. Particularly, the field of Social XR[462] might be considered within the sector of social networking services. XR-based entities like VRChat, Microsoft Mesh, Horizon Worlds, Echo VR or Rec Room offer various such Social XR services, allowing users from across the world to connect in a virtual space for shared experiences and communications.[463] Here, 'Social XR' refers to the linkage of XR technologies with communication platforms that merge the physical and virtual world to create simulate social interactions. Given these examples, XR-based entities offering online marketplace or social networking services could, if they trigger the relevant thresholds of the NIS2 Directive, be considered either 'Essential Entities' or 'Important Entities' under the NIS2 Directive and be subject to its obligations:

---

[459] Art. 6(28), NIS2 Directive read with Art 2(n), Directive 2005/29/EC, Unfair Commercial Practices Directive.
[460] Immersive Retail – Partner Solutions <https://aws.amazon.com/solutions/retail/immersive-retail/>; See also 'A guide to immersive retail & the metaverse age' (2022) Amazon Web Services <https://pages.awscloud.com/rs/112-TZM-766/images/Guide_to_Immersive_Retail_eBook_Final.pdf >
[461] Art. 6(33), NIS2 Directive.
[462] 'Social XR: Now and Future An exploration of Social XR Applications' TNO (2023) <https://publications.tno.nl/publication/34642231/2utunk/niamut-2024-social1.pdf>
[463] Michelle Cortese and Jessica Outlaw 'Social and Multi-User Spaces in VR: Trolling, Harassment, and Online Safety' (2021) IEEE Global Initiative on Ethics of Extended Reality (XR) Report <https://standards.ieee.org/wp-content/uploads/import/governance/iccom/social-multi-user-spaces-vr.pdf>

i. <u>XR services as 'Essential Entities':</u>

- <u>Based on size:</u> NIS2 Directive applies to private entities offering services listed in the Annex to the NIS2 Directive, provided that the entity exceeds the ceiling for medium-sized enterprises.[464] This would include entities employing over 250 persons, having an annual turnover over EUR 50 million, and having a balance sheet total over EUR 43 million[465] As of 2022, over 90% of all companies working on XR in Europe are reportedly SMEs.[466] Although the European XR market may reportedly grow to between €35 billion and €65 billion and may create 1.2 – 2.4 million jobs by 2025, these are projected figures, and may be applicable to XR-based services in the future upon reaching these thresholds.[467]
- <u>Based on critical function</u>: Regardless of size, the NIS2 Directive can also apply to entities playing a critical and significant role in a particular MS, as discussed in paragraph (2) of Section 1.2 above.[468] As discussed in Section 2.1(b) above, existing XR-based online marketplace and social networking services form a part of the Covered Digital Entities, and may therefore be categorized either as Essential Entities or as Important Entities under the NIS2 Directive. For such XR-based services to be essential entities, they must qualify based on size (discussed above). Alternatively, these entities must be:

  - the sole provider of services essential for maintaining critical societal or economic activities;
  - critically important at the national or regional level for its sector or other interdependent sectors; or
  - playing such a crucial role in that MS that any disruption to their services may cause a significant systemic risk, a significant impact on public health or security.

  This classification indicates that the purpose of designating essential entities regardless of size is to cover services that are extremely critical to a country's cyberspace and/or would significantly impact entire sectors, populations or the MS at large. Given the nature of XR-based services in the market, it is not clear if any such services would currently be covered within this categorisation.

ii. <u>XR services as Important Entities</u>: Any entity operating in the sectors mentioned in Annex I or Annex II, which is meeting the threshold of a medium sized enterprise and is not designated as an essential service by the MS, can be considered as an important entity.[469] Here, 'medium-sized enterprises' refer to those enterprises employing between 50 and 250 persons, having an annual turnover between EUR 10 million and EUR 50 million, and having a balance sheet total between EUR 10 million and EUR 43 million.[470]

[464] Art. 2(1), NIS2 Directive.
[465] Art. 2 of the Annex to Recommendation 2003/361/EC.
[466] European Commission 'Extended Reality- Shaping Europe's digital future' (2022) <https://digital-strategy.ec.europa.eu/en/policies/extended-reality>
[467] Ibid.
[468] Art. 2(2)- 2(4), NIS2 Directive.
[469] Art. 3(2), NIS2 Directive.
[470] Art. 2 of the Annex to Recommendation 2003/361/EC.

2.2 Obligations

The foregoing section analyses and sets out examples of entities that may be covered within the ambit of the NIS2 Directive. These entities would be required by MS to comply with the obligations discussed above in Section 1.3(2) to 1.3(8). These obligations could help minimize the extent of privacy and data protection harms and other potential harms caused by cybersecurity breaches and security incidents.[471]

However, these obligations would apply to those XR-based entities that both clear the medium-sized enterprise threshold of size, turnover and balance sheets, as well as offering services within specified sectors. The MS are required to publish a list of Covered Entities by 17 April 2025, and to update these lists at least every two years.[472] Publication of these lists would provide greater clarity on the extent to which XR-based services are subject to these obligations.

XR services present unique threats and vulnerabilities. This includes personal data breaches, user manipulation through processing of behavioural data and virtual identity theft- and shows the urgent need for enhanced security measures to protect the users and providers of XR services.[473] For example, researchers identify the following kinds of cybersecurity attacks possible through immersive VR spaces[474]:

(a) Overlay attack: an attack that overlays unwanted content on a user's VR overview;

(b) Chaperone attack: an attack that modifies the boundaries of the VR experience, making it appear smaller or larger;

(c) Disorientation attack: an attack used to elicit a sense of dizziness and confusion from the VR user;

(d) Human joystick attack: an attack that helps control the immersed user's physical movement, against their will, and move them to a different location; and

(e) Man-in-the-room attack: attacks that allow someone to infiltrate a chat room, extract information and even potentially manipulate the user's environment.

The nature of threats presented by XR-based services, particularly those enabling social interactions or allowing such new forms of cyber-attack vectors, may increasingly warrant greater cybersecurity protections. The NIS2 Directive primarily aims to address cybersecurity risks, cyber incidents and harms to users using the service covered by the NIS2 Directive. Given the extent of personal data processed by XR services and the extent to which users may be vulnerable to privacy harms, psychological harms or other harms[475], these obligations present an important layer of protection for XR users, in addition to protections listed in other EU legislations. However, there is reason to be concerned on whether these

[471] Emmie Hine et al 'Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations' (2024) < https://dx.doi.org/10.2139/ssrn.4585963 >
[472] Art. 3(3), NIS2 Directive.
[473] Melvin Abraham et al 'Implications of XR on Privacy, Security and Behaviour: Insights from Experts' (2022) Nordic Human-Computer Interaction Conference <https://doi.org/10.1145/3546155.3546691>
[474] Peter Casey, Ibrahim Baggili, Ananya Yarramreddy 'Immersive Virtual Reality Attacks and the Human Joystick' (2021) IEEE Transactions on Dependable and Secure Computing, 18(2) <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8675340 >
[475] As discussed extensively in XR4Human, Policy Report.

obligations are applicable to all the types of vulnerable XR services, given the limited scope of the NIS2 Directive.

7.3. Child Sexual Abuse Regulation

1. Overview

1.1 Background

Recent years have seen an increase in the use of digital platforms in perpetrating online child sexual abuse, through both the dissemination of child sexual abuse material (**CSAM**) and its use for solicitation of children for the purposes of child sexual abuse.[476] Currently, MS are obligated to ensure protection of children against sexual abuse, sexual exploitation, child pornography and solicitation of children for sexual purposes.[477] However, there is a need to address the use of digital platforms in the recording, disseminating or otherwise playing a role in child sexual abuse. In July 2020, the European Commission (EC) adopted the 'EU strategy for a more effective fight against child sexual abuse', aiming to, *inter alia*, enhance the reach of EU law in mitigating these harms on digital platforms.[478] As part of this strategy, the EU adopted Regulation 2021/1232 which permits providers of N-IICS to voluntarily adopt technical measures to detect CSAM or communications that solicitation of children.[479] This regulation does not create a legal obligation for N-IICS providers to implement these measures. Instead, it creates an exemption to pre-existing obligations on N-IICS providers to ensure the confidentiality and anonymity of communication data and traffic data under Directive 2002/58.[480] Additionally, Regulation 2021/1232 sets out safeguards in terms of proportionality and necessity, and imposes reporting obligations to competent authorities.[481] However, as these are merely voluntary measures, they may not be sufficient to address the extent of the harms caused by online child sexual abuse.

1.2 Scope

To address the role of digital platforms relating to online child sexual abuse, the EC has proposed the Regulation 2022/209 (**Child Sexual Abuse Regulation** or **CSAR**) laying down rules to prevent and combat child sexual abuse.[482] As of April 2024, the CSAR has been adopted by the European Commission, and has been sent to the European Parliament and the Council of the European Union, who have not yet declared their official position on this regulation. However, given that the CSAR is being designed as a *lex specialis* to the DSA[483], its provisions may be relevant in the context of XR technology, and is therefore being included in this review.

[476] Sample Cases of Child Sexual Abuse in the EU that originated from a report by an Online Service Provider <https://home-affairs.ec.europa.eu/document/download/22073d31-ed53-47b2-ba48-42e227cf3fa5_en?filename=Sample%20CSA%20cases%202019-2022.pdf> accessed 3 April 2024.
[477] Art. 3-7, Directive 2011/92
[478] European Commission, EU Strategy for a more effective fight against child sexual abuse <https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/eu-strategy-more-effective-fight-against-child-sexual-abuse_en#what-does-the-strategy-bring> accessed 3 April 2024
[479] Art. 3, Regulation (EU) 2021/1232.
[480] Art. 5(1) and 6(1), E-Privacy Directive
[481] Art. 3(1), Regulation 2021/1232.
[482] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, COM/2022/209 < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN> accessed 3 April 2024
[483] Recital 8, CSAR.

1.3 Subjects

The proposed CSAR will be applicable to providers of 'relevant information society services' (ISS), which include providers of hosting services, interpersonal communication services (ICS), software application services and internet access services, with a significant number of obligations being applicable to providers of hosting services and ICS.[484] In terms of the CSAR, 'hosting services' refer to all services that information provided by, and at the request of, a recipient of the service[485], and thus has a broader ambit than 'online platforms', as defined by the DSA, which cover hosting services that both store and disseminate information to the public at the request of the user.[486] Examples of hosting services include services such as cloud computing, web-hosting, paid referencing services, or services enabling sharing information and content online, including file storage and sharing.[487]

The obligations under the proposed CSAR shall be applicable to all covered providers offering ISS within the EU, irrespective of their place of main establishment.[488] However, such services need to have a substantial connection to the EU, either through a main establishment in the EU, through a significant number of users in the EU or by targeting activities towards one or more MS. [489] Mere technical accessibility of a website from the EU cannot be considered as establishing a substantial connection with the EU.[490] The CSAR does not specify a particular quantitative threshold for determining when the 'significant number of users' condition is met. For hosting services accessible from the EU and not covered by the CSAR, access to CSAM by users in the EU can be blocked through the internet access service providers.[491]

1.4 Main provisions

The CSAR broadly seeks to impose obligations on the relevant ISS providers, which include providers of hosting services and ICS, to undertake risk assessments, implement mitigation measures, and reporting and transparency obligations. Notably, the CSAR imposes certain obligations on specific types of providers of ISS such as hosting, ICS and software application stores. There are also some general obligations applicable to all covered ISS providers.

(a) General obligations imposed to all relevant ISS providers include:

i. Establish a point of contact[492] and to designate a legal representative if the provider is not based in the EU[493];

ii. Comply in a timely manner with the detection orders[494], blocking orders[495] and removal orders[496], as issued by the competent authorities under the CSAR; and

[484] Art. 1(1), CSAR.
[485] Art. 2(a), CSAR read with Art. 3(g)(iii), DSA.
[486] Art. 3(i), DSA.
[487] Recital 29, DSA.
[488] Art. 1(2), CSAR.
[489] Recital 11, CSAR.
[490] Ibid.
[491] Recital 32, CSAR.
[492] Art. 23, CSAR.
[493] Art. 24, CSAR.
[494] Art. 7-11, CSAR.
[495] Art. 16-18, CSAR.
[496] Art. 14-15, CSAR.

Funded by the European Union

iii. Cooperate and comply with both the investigatory and enforcement powers of the Coordinating Authorities, i.e., the agencies established by MS that ensure compliance with the CSAR.[497]

(b) Specific obligations imposed to ICS and hosting providers include:

i. Identify, analyse and assess the risk of each of their services being used for the purposes of online child sexual abuse.[498] For this, the providers must take into account:

- any previously identified instances of use of its services for the purposes of child sexual abuse;
- the manner in which users use the service, the manner in which the provider designed and operates the service, and the impact of these risks;
- the prohibitions under the services' terms and conditions and the measures implemented to enforce these prohibitions including functionalities on age-verification and flagging child sexual abuse; and
- the risks and functionalities associated with potential solicitation of children through these services.[499]

ii. Once these providers have identified risks through risk assessment, they are required to take reasonable mitigation measures tailored to those risks to minimize them.

- This may include, inter alia, adapting the provider's content moderation or recommender systems, decision-making processes, the functionalities of the service, or the content or enforcement of its terms and conditions, through appropriate technical and operational measures and staffing.[500]
- These mitigation measures must be targeted to the risk, applied in a proportionate and non-discriminatory manner taking into account the fundamental rights of all parties involved, the capabilities of the provider and the number of users, and must be reviewed in a timely manner.[501]
- An essential requirement under the CSAR is the obligation on providers of ICS to undertake age verification and age assessment measures that reliably identify child users on their services to implement the mitigation measures.[502]

iii. Report the process and results of the risk assessment undertaken, along with the mitigation measures taken pursuant to the risk assessment to the Coordinating Authority set up under the CSAR.[503]

iv. Report any information indicating child sexual abuse on its services[504];

[497] Art. 27-29, CSAR.
[498] Art. 3(1), CSAR.
[499] Art. 3, CSAR.
[500] Art. 4(1), CSAR.
[501] Art. 4(2), CSAR
[502] Art. 4(3), CSAR.
[503] Art. 5(1), CSAR.
[504] Art. 12, CSAR

v. Particularly, providers that receive a detection order, requiring a provider to detect online child sexual abuse in a particular service, must install and operate technologies that detect the dissemination of known or new CSAM or child solicitation.[505]

vi. Finally, providers of hosting services must provide reasonable assistance on request to EU residents seeking to remove or disable access to one or more specific CSAM item depicting them.[506]

(c) Specific obligations imposed to app stores: The CSAR imposes app stores to take reasonable steps to assess whether the services offered through the software applications present risks for being used to solicit children, to prevent child users from accessing such applications and to undertake age assessment measures to identify child users on their services.[507]

2. Applicability to XR technology

2.1 Subjects regulated within the XR ecosystem

As discussed above, the CSAR primarily seeks to impose obligations on providers of hosting services and ICS, while also imposing limited obligations on providers of software application store services and internet access services. We have previously discussed that XR technology would fall within the scope of the DSA given that most of these services would involve primarily hosting and disseminating information. Therefore, it is likely that if the CSAR were to be adopted in its present formulation, several XR technologies that offer services which primarily either involves hosting and disseminating information, or involves ICS, would be within the ambit of the CSAR. As discussed earlier, all providers of the relevant ISS "*offering such services in the Union*" are subject to the CSAR. However, the CSAR clarifies that a provider would not be said to *offer services* in the EU if it is merely technically accessible from the EU, and that the provider must either have their main establishment in the EU, failing which, if the provider of the ISS service has a significant number of users in the EU or targets their activities towards one or more MS.[508] There is little clarity on the quantitative threshold for what constitutes 'significant number of users' in the EU for services headquartered outside the EU. Comparatively, the DSA and the DMA clarify their respective thresholds for the number of users for VLOPs and VLOSEs, or for gatekeepers, at 45 million average monthly users.[509] However, any such XR-based provider with the main establishment in the EU would automatically be within the scope of this regulation.

Instances of virtual sexual assaults have been reported in the past as well, with a user in 2022 having been assaulted in Meta's Horizon Venues (now Horizon Worlds) by a group of male users within sixty seconds of joining the platform.[510] The issues of child sexual abuse and solicitation of children are particularly relevant in the XR-mediated world. Virtual reality creates avenues for newer forms of child sexual abuse. In January 2024, a 16-year-old girl playing a VR video game was subjected to a virtual gang-

[505] Art. 9(1), CSAR.
[506] Art. 21, CSAR.
[507] Art. 6(1), CSAR
[508] Recital 11, CSAR.
[509] Art. 33(1), DSA and Art. 3(2)(b), DMA.
[510] Maya Oppenheim, 'Woman reveals 'nightmare' of being 'gang raped' in virtual reality' (3 February 2022) Independent < https://www.independent.co.uk/news/uk/home-news/metaverse-gang-rape-virtual-world-b2005959.html > last accessed 5 April 2024.

rape through her digital avatar being assaulted by the avatars of other online players.[511] These instances, if recorded, raise the question of the extent of the proposed regulation in covering these actions.

Similarly, solicitation of children has been observed in the metaverse created by Roblox, a platform that allows users to create and play video games together, with a vast majority of its users being children. User-created sex games or 'condos' are spaces where users can talk about sex or their characters can have virtual sex, operating outside Roblox's rules.[512] These spaces can also be used by adults for solicitation of children or 'grooming', with the Canadian Centre for Child Protection issuing a warning on this issue in 2017.[513] These existing issues and threats to child safety in existing metaverse services raise concerns regarding the impact of XR-based metaverse spaces that offer greater immersion for its users. Providers of hosting services and interpersonal communication services mediated through XR technologies are therefore likely to be subject to these regulations based on whether they are based in the EU or offer services to a 'significant' number of EU residents.

2.2 Obligations for XR providers

In terms of XR technology, providers of VR-based games, services that allow users to engage in interpersonal communication, and XR-based services that allow the hosting of content for users are likely to be responsible for the bulk of the provisions under the CSAR. The CSAR aims to impose risk assessment obligations on all such providers, to assess the risks of its services being used for the purposes of child sexual abuse or for solicitation of children. For example, a recent instance in Egypt involved a person advertising the sale of CSAM pictures and videos, shot through a 360-degree camera, was being offered for sale through VR.[514] The CSAR's obligations are particularly relevant in instances such as these, where the CSAM can be hosted on VR headsets prior to being offered for sale to third parties. The covered providers under the CSAR must assess the risks of their services being used in this manner and take measures to mitigate these risks in line with the risk mitigating obligations imposed by the CSAR.

An XR-based ISS provider may be notified via a detection order of the existence of child sexual abuse or child solicitation on their services, or of the use of their services for child sexual abuse or child solicitation. In such cases, the provider would be required to implement appropriate technical and organizational measures to identify and detect CSAM dissemination or child solicitation.

Another major obligation relevant to XR-based multiplayer video games relying on the concept of metaverses is the issue of identifying the ages of individual users and preventing adult users from being able to solicit children for sexual purposes. Particularly, there are app stores tailored to VR technology, offering VR games, fitness apps, and social apps connectable to the VR headsets.[515] In 2024, Apple

---

[511] Snejana Farberov, 'Police investigating first case of girl's virtual gang rape in metaverse' (2 January 2024) The New York Post <https://nypost.com/2024/01/02/news/police-investigating-first-case-of-virtual-rape-in-metaverse/> last accessed 5 April 2024.
[512] James Clayton and Jasmin Dyer, 'Roblox: The children's game with a sex problem' (15 February 2022) BBC < https://www.bbc.com/news/technology-60314572 > last accessed 5 April 2024.
[513] 'Child protection group warns parents about luring, explicit chat on game site Roblox' (24 February 2017) CBC News < https://www.cbc.ca/news/canada/manitoba/winnipeg-roblox-luring-warning-1.3997258 > last accessed 5 April 2024.
[514] Angus Crawford, 'Child abuse material found on VR headsets, police data shows' BBC (22 February 2023) < https://www.bbc.com/news/uk-64734308> last accessed 5 April 2024.
[515] Examples include Meta's Quest VR shop < https://www.meta.com/en-gb/experiences/?utm_source=exp_hub_nav&utm_medium=self_referral > last accessed 5 April 2024; and Viveport's Infinity Subscription < https://www.viveport.com/ > last accessed 5 April 2024.

Funded by the European Union

announced that its MR headset Vision Pro was going to be launched in the US, with the App Store pre-installed in the headset featuring more than 600 apps and games specifically designed for Vision Pro.[516] This would be considered a software application store, and Apple may be required to assess the risk of solicitation for each of these applications, preventing child users from accessing applications that pose a significant risk, and taking the necessary age-verification and age-assessment measures to reliably identify child users.[517]

[516] 'Apple announces more than 600 new apps built for Apple Vision Pro' (1 February 2024) Apple Newsroom < https://www.apple.com/newsroom/2024/02/apple-announces-more-than-600-new-apps-built-for-apple-vision-pro/> last accessed 5 April 2024.
[517] Art. 6, CSAR.

Funded by the European Union

8. Accessibility and non-discrimination

8.1. European Accessibility Act

1. Overview

1.1. Scope

The European Accessibility Act (EAA; Directive 2019/882), enacted by the European Parliament and the Council of the European Union on April 17, 2019, is designed to "contribute to the proper functioning of the internal market by facilitating the harmonization of the laws, regulations, and administrative provisions of the MS with regard to accessibility requirements for certain products and services." This objective is to be achieved, in particular, through the elimination and prevention of barriers to the free movement of certain accessible products and services that arise from divergent accessibility requirements in the MS. This would result in an increased availability of accessible products and services within the internal market, as well as an enhanced accessibility of pertinent information (Art. 1). The principal objective of the directive is, therefore, to harmonize the country-specific legal regulations within the EU, thereby ensuring a greater availability of accessible products and services. In consequence, the EAA is principally directed towards manufacturers, importers, and service providers, in addition to a lesser extent towards users.

1.2. Subjects

The provisions of this directive apply to manufacturers, importers, distributors, and service providers in all MS. This encompasses entities that operate products or services within the EU, even in the absence of a registered office within the EU. In order to achieve this objective, Article 3 provides a comprehensive delineation of the relevant terms. Furthermore, the directive defines persons with disabilities as individuals who experience long-term physical, mental, intellectual, or sensory impairments, which, when coupled with various barriers, may impede their full and effective participation in society on an equal basis with others[518].

1.3. Main provisions

This Directive outlines the regulatory framework for various products and services placed on the market and provided to consumers after 28 June 2025. These include[519]:

- Consumer General Purpose Computer Hardware Systems and Operating Systems
- Self-Service Terminals:
  - Payment Terminals
  - Self-Service Terminals dedicated to services such as:
    - Automated Teller Machines (ATMs)
    - Ticketing Machines
    - Check-in Machines
    - Interactive Information Terminals (excluding those integrated into vehicles, aircraft, ships, or rolling stock)

[518] See Article 3 (1)
[519] See Art. 2

- Consumer Terminal Equipment with Interactive Computing Capability used for:
    - Electronic communications services
    - Accessing audiovisual media services
- E-readers
- Electronic Communications Services, excluding transmission services for machine-to-machine communications
- Access to Audiovisual Media Services
- Passenger Transport Services (air, bus, rail, waterborne), with specified exceptions:
    a. Websites
    b. Mobile applications
    c. Electronic tickets and ticketing services
    d. Real-time travel information (interactive screens within the EU only)
    e. Interactive self-service terminals (excluding integrated terminals in vehicles, aircraft, ships, rolling stock)
- Consumer Banking Services
- E-books and Dedicated Software
- E-commerce Services

Emergency Communications:

- Applicable to answering emergency communications to the European emergency number '112'.

It is important to note, however, that no explicit technological specifications are ever provided. The directive merely requires that accessibility be provided in accordance with the specifications outlined in Annex I. For example, information regarding the utilization of the product or service must be accessible and intelligible via a multitude of sensory channels. Moreover, user interfaces and functional design must be constructed in a way that guarantees the availability of alternative access options for all sensory perceptions. Moreover, interfaces for assistance systems and devices are required, such as personal headsets. The default configuration must facilitate access to these barrier-free options, which should not necessitate user intervention. Section VII provides a comprehensive list of functional performance criteria, including usability for individuals with vision, colour perception, hearing, vocal capability, limited manipulation or strength, limited reach, and cognitive limitations. Furthermore, measures must be taken to minimize the risk of triggering photosensitive seizures and ensure usability for individuals with limited cognition. The overall privacy of the user must be maintained.

1.4. Rights and obligations

Manufacturers are obliged to[520]:

a) **Design and Manufacturing Compliance**: Ensuring products meet accessibility requirements when placed on the market.
b) **Technical Documentation and Conformity Assessment**: Preparing documentation per Annex IV, conducting conformity assessments, and issuing the EU declaration of conformity and CE marking.
c) **Record Keeping**: Retaining technical documentation and the EU declaration of conformity for five years post-market placement.
d) **Ongoing Conformity**: Maintaining conformity during series production, considering design changes and updated standards.

[520] See Article 7

e) **Product Identification**: Marking products with identifiable information (type, batch, or serial number) or providing it on packaging/documents.
f) **Manufacturer Identification**: Indicating the manufacturer's name, trade name, trademark, and contact address on the product or its packaging/documents.
g) **Instructions and Safety Information**: Providing clear, understandable instructions and safety information in the relevant language.
h) **Corrective Measures and Reporting Non-compliance**: Taking immediate action to correct or withdraw non-compliant products and informing national authorities of non-compliance details.
i) **Cooperation with Authorities**: Providing necessary information and documentation to national authorities and cooperating to resolve non-compliance issues.

Authorized representatives appointed by manufacturers maintain compliance documentation, provide necessary information, and cooperate with authorities on non-compliance actions[521].

The responsibilities of importers and distributors consist of[522]:

- **Market Placement Compliance**:
  - Importers and distributors must ensure products meet accessibility standards before market placement.
  - Verify manufacturers have completed the conformity assessment in Annex IV, prepared necessary technical documentation, and affixed the CE marking.
  - Importers must ensure products are accompanied by required documentation and comply with Article 7(5) and (6) and Article 9(4).
- **Non-Compliance Actions**:
  - If importers suspect non-compliance, they must withhold the product from the market until compliant and inform the manufacturer and relevant authorities.
  - Product and packaging labels must include contact details understandable to end-users and authorities.
  - Importers must provide instructions and safety information in an accessible language.
  - Ensure storage and transport conditions do not affect compliance, keep the EU declaration of conformity for five years, and take corrective actions or withdraw non-compliant products.
  - Inform national authorities of non-compliance, maintain a register of such products and complaints, provide necessary documentation to authorities upon request, and cooperate on compliance actions.

The role of the market surveillance authorities can be defined as follows[523]:

- **Evaluation and Enforcement**:
  - Authorities will evaluate suspected non-compliant products and economic operators must cooperate.
  - If non-compliance is found, operators must correct it within a set period or withdraw the product.
  - Authorities will notify the Commission and other MS if non-compliance may affect other regions.
  - Operators must apply corrective actions to all non-compliant products across the EU.
  - If operators fail, authorities will take provisional measures to prohibit, restrict, or withdraw the product and inform the Commission and other MS.

[521] See Article 8
[522] See Article 9 and 10
[523] See Article 19 and following

- Shared information will include product details, non-compliance nature, measures taken, and operator arguments.
- Other MS must report any measures taken and objections within three months, after which provisional measures are deemed justified.
- MS must promptly enforce restrictive measures, such as product withdrawal, for non-compliance.

It is important to note that the EAA is not yet in force; however, there is a transition period until 28 June 2025. In the interim period, organizations are afforded the opportunity to ensure that all of their products and services comply with the EAA. Furthermore, the regulation does not apply to companies with fewer than 10 employees and a turnover of less than two million EUR per year.

It is incumbent upon companies within the EU and those outside the EU that offer or sell products in the EU to ensure that all products are brought into compliance with the EAA. In the event of non-compliance, penalties may be imposed, contingent on the gravity and nature of the infraction. Moreover, MS are obliged to conduct periodic compliance audits and to examine and address grievances. Additionally, MS must establish centralised bodies to oversee, enforce and impose sanctions on violations. These bodies are also tasked with acting as points of contact for complaints.

Moreover, all products must be affixed with a CE marking. The CE marking must adhere to the overarching principles delineated in Article 30 of Regulation (EC) No 765/2008. The CE marking must be affixed in a manner that is both visible and legible, and in a location that is indelible on the product or its data plate. In the event that affixing the CE marking to the product itself is not feasible due to the product's nature, it must be placed on the packaging and accompanying documents. The CE marking must be applied before the product is placed on the market. MS are responsible for ensuring the correct application of the CE marking regime and must take appropriate action in cases of improper use, using existing enforcement mechanisms. This Directive aims to standardize the CE marking process to ensure product compliance while minimizing administrative burdens on small businesses.

2. Applicability to XR

The EAA serves to enhance accessibility for a range of products and services, including those pertaining to XR technologies, which encompass VR, AR and MR systems. The EAA requires that XR devices and their software comply with the requisite accessibility standards to ensure usability for individuals with disabilities. XR devices are initially classified as consumer hardware with interactive computing capabilities, and their software must comply with the relevant accessibility standards. In addition, applications that provide audiovisual media, e-books, e-commerce, and other interactive services must be designed in a manner that ensures accessibility for users with visual, auditory, and motor impairments. Moreover, XR devices and applications are required to provide alternative input methods, such as voice commands and eye-tracking, and offer customizable settings, including text size and colour contrast. The latest generation of XR technologies and applications, exemplified by the Meta Quest and the Apple Vision Pro, have already incorporated accessibility settings within their VR headsets. It is also of paramount importance that XR technology is compatible with assistive technologies, including screen readers, hearing aids, and alternative input devices, in order to guarantee full interaction with XR environments. Furthermore, real-time information services in XR applications, such as transport information, must be accessible through features like text-to-speech options, sign language interpreters, or visual alerts. In terms of compliance, it is the responsibility of manufacturers to ensure that their XR products meet the requisite EAA accessibility requirements and obtain the CE marking, which signifies compliance. Moreover, a declaration of conformity must be provided, detailing how accessibility standards are met and identifying any exceptions. It is the responsibility of the MS to ensure market compliance, with penalties or removal from the market for products that do not comply with the relevant standards. In the context of XR product development and design, it is of the utmost importance that accessibility considerations are integrated from the outset. This necessitates the implementation of user testing with individuals who are disabled and the adherence to accessibility guidelines, such as WCAG. Moreover, organizations must provide training to their teams on accessibility best practices and EAA requirements, with the dual objective of ensuring compliance and enhancing the user experience. The overarching objective of the EAA is to ensure the inclusivity and accessibility of XR technologies, thereby facilitating equal access to digital innovations for all individuals.

Funded by the European Union

8.2. Web Accessibility Directive

1. Overview

1.1. Scope

The **Web Accessibility Directive** (Directive 2016/2102) ("**WAD**") was formally adopted by the European Parliament and the Council on October 26, 2016. The directive entered into force on December 22, 2016. MS were required to transpose the directive into national law by September 23, 2018, in accordance with the established timeline for implementation. New public sector websites published after September 23, 2018, had to be compliant by September 23, 2019. Existing public sector websites published before September 23, 2018, were required to comply by September 23, 2020. Additionally, public sector mobile applications needed to be compliant by June 23, 2021.

1.2. Subjects

The WAD is applicable to all MS, in addition to those belonging to the EEA. The directive addresses the following subjects:

(a) **Digital Accessibility for Public Sector**: Ensuring websites and mobile applications of public sector bodies are accessible to all users, especially people with disabilities.

(b) **Common Accessibility Requirements**: Establishing common accessibility standards.

(c) **Accessibility Statements**: Requiring public sector bodies to publish accessibility statements detailing the accessibility status of their websites and mobile applications.

(d) **Feedback Mechanism**: Implementing a feedback mechanism for users to report accessibility issues and request accessible information.

(e) **Monitoring and Reporting**: Regular monitoring of the accessibility of public sector websites and mobile applications and reporting the results to the European Commission.

(f) **Harmonization and Standardization**: Harmonizing national measures and standards to reduce fragmentation in the internal market, fostering interoperability and innovation.

(g) **Training and Awareness**: Promoting awareness and training programs related to web accessibility for relevant stakeholders, including public sector staff.

(h) **Support for SMEs**: Addressing the needs of small and medium-sized enterprises (SMEs) in the accessibility market to enhance their competitiveness and reduce market entry barriers.

(i) **Economic and Social Benefits**: Ensuring that public sector bodies and enterprises gain economic and social benefits from making their digital services accessible to more citizens and customers.

(j) **Universal Design and Assistive Technologies**: Encouraging the design of products, environments, programs, and services to be usable by all people without the need for adaptation or specialized design, while also allowing for assistive devices for particular groups of persons with disabilities.

(k) **Inclusion of Various Content Types**: Covering textual and non-textual information, downloadable documents and forms, and two-way interaction such as digital forms and authentication processes.

(l) **Exemptions and Special Cases**: Providing temporary or permanent exclusions for certain types of content, like live time-based media or third-party content, while encouraging accessible alternatives where possible.

(m) **Stakeholder Consultation**: Consulting relevant stakeholders, including organizations representing the interests of persons with disabilities, industry representatives, and civil society, to ensure effective implementation of the directive.

(n) **Review and Update Mechanisms**: Establishing procedures for reviewing and updating the directive's requirements in light of technological advances and feedback from stakeholders.

By addressing these subjects, the directive aims to ensure that public sector digital services are accessible to all, promoting inclusivity and equal access to information and services across the European Union.

1.3. Main provisions

The WAD aims to enhance the accessibility of public sector websites and mobile applications across the European Union. This directive applies to all public sector bodies, including websites and mobile applications, with the exception of those engaged in broadcasting and certain non-governmental organizations that do not provide essential services. In line with the requirements of this directive, digital services must comply with the accessibility criteria set out in the European standard EN 301 549 V2.1.2, which aligns with the Web Content Accessibility Guidelines (WCAG) 2.1 at level AA[524]. The Web Content Accessibility Guidelines (WCAG) 2.1 at level AA are a set of guidelines developed by the World Wide Web Consortium (W3C) with the objective of making web content more accessible to people with disabilities. These guidelines build on the foundation set by WCAG 2.0 and include additional success criteria to address more accessibility barriers. The key components and principles of WCAG 2.1 at level AA are as follows:

(a) **Perceivable**: It is essential to present information and user interface components in ways that can be perceived by users. This entails providing text alternatives for any non-text content, such as images and videos, so that the information can be converted into other forms that people require, including large print, braille, speech, symbols, or simpler language. For time-based media, alternatives must be provided, including captions for videos and audio descriptions for visual content. Furthermore, content should be adaptable, meaning it can be presented in different ways, such as with a simpler layout, without losing information or structure. Additionally, content must be distinguishable, making it easier for users to see and hear by separating the foreground from the background.

(b) **Operable**: It is essential that user interface components and navigation are fully operational. This entails guaranteeing that all functionality is accessible via keyboard, thus enabling users who are unable to use a mouse to navigate and interact with the site. It is also essential to allow users sufficient time to read and utilise the content, ensuring that those who may require additional time to process information are accommodated. Furthermore, content should be designed in a way that does not cause seizures, in order to ensure the safety of users with photosensitive conditions. To facilitate navigation, it is essential to provide users with the necessary tools to locate content and comprehend their position within the site. Finally, functionality should be operable through various input modalities beyond the keyboard, such as touch and voice, in order to accommodate different user preferences and needs.

[524] Article 6, WAD

(c) **Understandable**: The information provided and the operation of the user interface must be clearly understood. This entails ensuring that text content is both readable and comprehensible, allowing users to easily grasp the information presented. It is essential that web pages appear and operate in a predictable manner, allowing users to anticipate how they will interact with the site and navigate through it consistently. Furthermore, input assistance should be provided to assist users in avoiding mistakes and correcting them when necessary, thereby enhancing the overall usability and user experience.

(d) **Robust**: Content must be robust enough to be reliably interpreted by a wide variety of user agents, including those with assistive technologies. This entails optimizing compatibility with existing and emerging user agents to guarantee that all users, irrespective of their technology preferences, can access and interact with the content in an effective manner. To guarantee robust content, it is essential to utilise standardised coding practices and technologies that facilitate seamless integration with assistive devices, thereby ensuring an inclusive digital experience for all users.

In accordance with the WAD, public sector bodies are bound by law to provide and regularly update an accessibility statement for their digital services[525]. Such statements must delineate the degree of compliance, identify any instances of inaccessible content, and elucidate the rationale behind such inaccessibility, if applicable. Furthermore, a feedback mechanism must be incorporated into the design of the digital service, through which users can report any accessibility issues and request information in accessible formats. Furthermore, the directive exempts specific categories of content from these obligations, including office file formats published prior to September 23, 2018, live audio and video content, and online maps and mapping services, provided that essential information is accessible. Furthermore, the directive excludes third-party content that is not funded or controlled by the public sector body in question. With respect to monitoring and enforcement, the responsibility for regular monitoring of the compliance of public sector websites and mobile applications and for submission of findings to the European Commission on a triennial basis (commencing December 23, 2021) falls upon the MS. The methodology and results of the monitoring process must be made publicly accessible. In order to guarantee compliance with the directive, MS are required to implement penalties that are effective, proportionate, and dissuasive for instances of non-compliance. This ensures that users are able to submit effective complaints. Moreover, the directive recommends the implementation of training programs, technical assistance, and awareness-raising activities to facilitate the attainment of compliance by public sector bodies. Moreover, it encourages collaboration between MS with the objective of disseminating exemplary practices and resources. In conclusion, these measures ensure a uniform and elevated degree of accessibility throughout the EU, thereby advancing inclusivity and equal access to information and services for all citizens, including those with disabilities.

1.4. Rights and obligations

Public sector bodies must regularly provide a detailed, comprehensive and clear accessibility statement on how their websites and mobile applications comply with this directive, including:

i. an explanation for any inaccessible elements and information on accessible alternatives;
ii. a description on how a user may report any failure to comply with this directive or request information that is excluded from the scope of this directive;
iii. a link to a complaint mechanism that can be used if the response is inadequate.

[525] Article 7, WAD

Implementing Decision (EU) 2018/1523, an implementing act adopted by the European Commission, establishes a model accessibility statement.

MS must also:

i. facilitate the application of the accessibility requirements to other types of websites and mobile applications covered by existing national laws;
ii. facilitate training programs on the accessibility of websites and mobile applications;
iii. raise awareness of the accessibility requirements;
iv. share best practice, facilitated by the Commission;
v. ensure the availability of an effective enforcement procedure.

MS may maintain or enact legislation which goes beyond the minimum requirements of this directive. This directive does not apply to public service broadcasters or non-governmental organizations that do not provide services that are essential to the public or specifically to people with disabilities. In addition, it does not apply to the following content elements:

i. office file formats published before 23 September 2018, unless needed for administrative processes by the public sector body concerned;
ii. audio or video published before 23 September 2020;
iii. live audio or video;
iv. online mapping, as long as essential navigational information is provided in an accessible manner;
v. third-party content not under the control of the public sector body concerned;
vi. reproductions of heritage items or manuscripts in certain circumstances;
vii. extranet and intranet content intended for a closed group of people, published before 23 September 2019, until they have a major update;
viii. content of websites and mobile applications not updated or edited after 23 September 2019 (archives), if their content is not needed for administrative processes.

MS may exclude the websites and mobile applications of schools, kindergartens, or nurseries, except for content relating to essential online administrative functions. It is the responsibility of MS to monitor the compliance of websites and mobile applications of public sector bodies with the accessibility requirements on a regular basis. By December 23, 2021, and every three years thereafter, MS shall submit to the Commission a report on the outcome of the monitoring, including the measurement data.

2. Applicability to XR

2.1. Scope

The WAD primarily focuses on ensuring that websites and mobile applications of public sector bodies are accessible. However, as the use of XR technologies, including VR and AR, becomes more prevalent in public services, it is important to consider the directive's implications for XR applications. While the directive does not explicitly mention XR technologies, the general principles of accessibility—making content perceivable, operable, understandable, and robust—apply to all digital content and services. Public sector bodies utilizing XR technologies must ensure these applications are accessible to users with disabilities, following similar principles to those outlined for websites and mobile applications. XR applications that provide public services or information fall within the directive's scope, particularly if they are part of the public sector bodies' digital offerings. For example, a public museum using VR for virtual tours must ensure these tours are accessible, including features like audio descriptions and navigable interfaces.

Funded by the European Union

While there are no specific standards for XR in the directive, public sector bodies can refer to existing accessibility guidelines, such as the Web Content Accessibility Guidelines (WCAG) 2.1, and adapt them to XR environments. Standard bodies and organisations like the World Wide Web Consortium (W3C) and XR Access are developing best practices for accessibility in XR, which can inform public sector bodies' compliance efforts. Public sector bodies using XR technologies should include information about the accessibility of these applications in their accessibility statements. This includes detailing any accessibility features, known barriers, and how users can provide feedback or request accommodations. Similar to websites and mobile applications, XR applications should have mechanisms for users to report accessibility issues and request accessible alternatives.

2.2. Challenges and Considerations

(a) **Technical and Design Challenges**:

- Ensuring XR applications are accessible involves addressing unique challenges, such as providing alternative text for visual elements in VR or ensuring AR content is perceivable by users with visual impairments.
- Designing intuitive navigation and control mechanisms for users with different abilities is crucial.

(b) **Emerging Standards and Best Practices**:

- As XR is an emerging technology, standards and best practices for accessibility are still developing.
- Public sector bodies should stay informed about advancements in XR accessibility and incorporate these practices into their applications.

(c) **User Experience and Testing**:

- Inclusive design and thorough user testing with people with disabilities are essential to identify and address accessibility barriers in XR applications.

While the WAD does not explicitly address XR technologies, the principles and obligations it sets forth for digital accessibility apply broadly to all public sector digital content and services. Public sector bodies incorporating XR technologies should ensure these applications are accessible by following existing accessibility guidelines, adapting emerging best practices, and providing clear accessibility information and feedback mechanisms. This approach will help meet the directive's goals of inclusivity and equal access to public services for all users, including those with disabilities.

9. Artificial Intelligence Act

1. Overview of the regulation

1.1. Scope

The Regulation 2024/1689 "Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts" or **AI Act** is a regulation that was introduced in April of 2021. Overall, it presents the first regulatory framework for artificial intelligence with a comprehensive approach, aiming to foster human-centric and trustworthy AI[526]. In general, the AI Act aims to create a regulation which weighs the benefits of AI's development with the challenges of protecting individuals as well as societies. The overall principle can be summed up as: fostering an environment in which AI can develop responsibly and ethically.

The main objective of the AI Act is to regulate the placing on the market, the putting into service, and the use of AI systems.[527] AI systems are defined as "machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".[528]

1.2. Subjects

The AI Act aims to regulate a broad number of entities involved in the development, deployment, and use of AI systems. This includes, among others: providers (developers) of AI systems, deployers (individuals or organizations that use an AI system), importers of AI systems from outside the EU, and distributers that make AI systems available and are not the original providers.[529] These entities should ensure that the AI systems comply with the regulatory requirements (especially if classified high-risk) and/or that use is in accordance with the intended purpose.

Other important actors include: authorized representatives that are appointed by providers established outside the EU to act on their behalf in ensuring compliance. Conformity assessment bodies are independent organizations designed to assess if high-risk AI systems meet the requirements and can issue certifications. National competent authorities are public bodies in all MS that are responsible for supervising the enforcement of the AI Act by overseeing compliance, dealing with complaints and enforcing actions. The European Artificial Intelligence Board (EAIB) is a central body that coordinates the implementation across the EU. It gives guidance, facilitates cooperation among national authorities and ensures consistency in the application of the Act. Overall, these entities represent the whole lifecycle of AI systems: from development to use.

1.3. Main provisions

Among the main provisions of the AI Act are the following ones:

---

[526] Article 1, AI Act
[527] Article 1 (2)(a), AI Act
[528] Article 3(1), AI Act
[529] Article 3(3), (4), (6), (7) AI Act.

(a) **Comprehensive Scope**: The AI Act is one of the first attempts globally to create a broad and comprehensive set of regulations specifically for AI systems. It covers the entire lifecycle of AI, from development to deployment and use, addressing various stakeholders involved.

(b) **Risk-Based Approach**: Uniquely the AI Act aims to categorize AI systems according to the level of risk they pose to health, safety, and fundamental rights of individuals. This classification into risk levels in turn determines the regulatory requirements that then apply. These risk categories range from:

- **Unacceptable risk**[530]: systems are considered a clear threat, such as social scoring by governments, certain types of biometric identification in public spaces. These systems are prohibited outright. An example of this is an application that exploits vulnerabilities of specific groups, such as children or people with disabilities, by using their behavioural data to manipulate decisions or actions that may lead to harm. This could also be relevant for XR applications, as these can for instance use data of children that could unintendedly manipulate behaviour.
- **High risk**[531]: systems that pose significant risk to safety or basic rights, such as those used in critical infrastructures as well as educational training (exam scoring), law enforcement, border control management. These systems must undergo rigorous conformity assessments and follow transparency and accountability measures and maintain proper documentation and logging while ensuring human oversight. An example of this is predictive policing, so AI systems that are used to predict criminal activities and allocate law enforcement resources. Another high risk application would be AI used in education, in which AI systems are used to assess students (such as automated grading systems) which could impact students' future opportunities. These systems must be transparent, fair, and accurate to avoid biases and unfair treatment. For XR applications used in educational settings this risk category can be relevant if they for instance score students during the use.
- **Limited risk**: systems with a lower risk must adhere to specific transparency obligations, such as systems that interact with humans, emotion recognition systems and biometric categorization systems. The providers must inform users about interactions with AI and give adequate information about the functioning of the systems. An example for a limited risk application is a customer service chatbot. These AI-powered chatbots can be implemented by companies to interact with customers. These chatbots are designed to provide information, answer queries, or help with basic tasks such as booking appointments or handling customer complaints. In this case it would be important for the customer to know that they are interacting with an AI system.
- **Minimal risk**: systems that pose minimal or no risk to users' rights or safety, which include AI-enabled spam filters or entertainment systems. Compliance is mainly based on voluntary codes of conduct and best practices. An example here is spam filters for email. Here AI systems are used to automatically detect and filter out spam messages from users' inboxes. These systems analyse email content and patterns to identify and separate unwanted emails from legitimate ones.

Overall, with these risk categories the AI Act aims to apply a balanced and proportionate level of regulation and scrutiny to the systems.

[530] Recital 31, AI Act
[531] Article 6, AI Act

(c) **Focus on Fundamental Rights and Ethical Use**:

- Emphasizes protecting fundamental rights, such as privacy, non-discrimination, and human dignity, by embedding these principles into the regulatory framework.
- Encourages the ethical development and deployment of AI, reflecting European values and societal concerns.

(d) **Transparency and Accountability Requirements**:

- Mandates transparency measures, such as clear labelling of AI systems, especially those interacting with humans. Users must be informed when they are interacting with AI.
- Requires accountability mechanisms, including human oversight and documentation to ensure AI systems can be audited and scrutinized.

(e) **Extraterritorial Reach**: Applies not only to AI systems developed and used within the EU but also to those outside the EU if they affect people within the EU. This extraterritorial scope is aimed at ensuring that the regulations have a broad impact on global AI practices.

(f) **Innovation-Friendly Provisions**:

- Includes regulatory sandboxes to foster innovation by allowing companies to test and develop AI systems in a controlled environment under regulatory supervision.
- Aims to balance regulation with the need to support technological innovation and maintain Europe's competitiveness in the AI sector.

(g) **Governance and Oversight**:

- Establishes a structured governance framework with the creation of a European Artificial Intelligence Board (EAIB) to facilitate consistent implementation across MS.
- National supervisory authorities will oversee compliance and enforcement within their jurisdictions.

(h) **Mandatory Conformity Assessments**:

- High-risk AI systems must undergo rigorous conformity assessments before being placed on the market. These assessments ensure that systems meet safety and performance standards.
- Regular post-market monitoring and reporting requirements are also mandated for high-risk AI systems.

The EU AI Act is distinctive because it represents a proactive and holistic approach to AI regulation, aiming to shape the development and use of AI in a way that is both innovative and aligned with European values and legal standards.

2. Applicability to XR

The AI Act may apply to XR providers that use AI systems in their software or platforms. The definition of AI system includes those which have an impact in virtual environments. For instance, AI-powered XR applications that use AI algorithms for object recognition, spatial mapping, gesture recognition or language processing could fall under the scope of the AI Act. The obligations that such an XR provider will have to comply with will depend on whether it is classified as a developer of an AI system or a deployer of an AI system, with the latter being more likely.

Overall, the risk assessment approach of the AI Act bears the possibility that some XR applications could be regarded as "unacceptable risk" and thus prohibited since they may alter realities and perceptions of people, including vulnerable groups, such as children, or the applications that use of 'real-time' remote biometric identification systems through XR devices (e.g. headsets).

Further, any other acceptable use of AI systems on XR applications will need to comply with several obligations:

- The AI Act's focus on transparency and accountability in the development and deployment of AI systems would mean that XR applications with AI functions should be transparent about the capabilities, limitations and potential biases. Therefore, XR developers may have to provide explanations how AI algorithms function. This is especially relevant if these algorithms highly impact users' experiences of decisions within XR environments. Overall, traceability varies considerably and AI developers do not have capabilities to trace back decision, especially AI models types such as deep learning or regarding the complexity of the applied model. If XR applications use these models of AI then transparency and accountability become impossible to ensure.
- Safety and security standards are another issue that must be ensured in XR applications with AI components, to minimize risks to users and prevent malicious use. This includes that AI-powered XR technologies are robust, reliable and resistant to misuse. Issues of cyber security and AI systems
- Overall, the Act aims to promote ethical considerations in the development and use of AI. This also applies to XR technologies that incorporate AI as these must adhere to ethical principles such as fairness, transparency, accountability and human oversight. These different issues are relevant for both providers and users. In general, while the EU's AI Act primarily targets AI technologies, its regulatory framework can indirectly impact XR applications that utilize AI algorithms, shaping the development, deployment, and usage of AI-powered XR experiences within the European Union. The European Commissions AI ethics guidelines[532] do not explicitly include XR, so it will remain a challenge to see whether these guidelines can be operationalized for XR applications (such as ethics by design).

Challenges for XR implementation can be identified in the main critique points of the AI Act itself. Its risk-based approach and categorization into risk levels is regarded by some are too complex and confusing in implementation and enforcement. Therefore, it might be difficult or unclear for some XR technologies using AI components in which risk level they fall. This in turn can lead to confusion regarding the regulatory requirements and could slow down development of the technologies. Also, possible suppression of experimental research can also influence the development of XR technologies.

In general, compliance with the AI Act's requirements can pose a significant burden on XR business that produce or deploy AI features, including SMEs, regarding costs and administration. This is tied to concerns that the strict regulations could suppress innovation in AI in the EU and hinder experimentation. This is related to issues of international competitiveness (competitive disadvantage of EU companies) and research on AI that could be influenced by restrictions on certain AI applications[533].

532 https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
533 https://www.politico.eu/article/eu-commission-innovation-shush-ai-act-critics/

However, complying with the AI Act can also help the European XR market to be positioned as uniquely trustworthy and ethical in comparison with other jurisdictions.

10. Health law

1. Medical Devices Regulation

1.1. Scope

All medical devices intended for use in the European Union are subject to the Medical Device Regulation (EU) 2017/745. This regulation was enacted by the European Parliament on April 5, 2017, and was most recently extended on March 20, 2023, in response to the ongoing pandemic. The primary objective of the regulation is to harmonise and guarantee the quality of medical products and associated clinical studies. This ensures a functioning internal market for medical devices within the EU, while protecting the health of users and patients. It should be noted that the MDC encompasses not only medical products but also a range of other items used on or in the human body. This includes non-medical devices listed in Annex XVI, such as contact lenses, devices for transcranial stimulation of the brain, and cosmetic products. The regulation also explicitly addresses the use of clinical studies, which form the basis for medical devices.

1.2. Subjects

In order to establish a general consensus, Article 2 of the MDC provides a list of valid definitions of the individual terms. In this regard, a "medical device" is defined as "an instrument, apparatus, appliance, software, implant, reagent, material, or other article which, according to the manufacturer, is intended for human use and which, alone or in combination, is intended to fulfil one or more of the following specific medical purposes:

The following are examples of medical devices:

- diagnostic, preventative, monitoring, predictive, prognostic, therapeutic, or palliative devices for disease;
- diagnostic, monitoring, therapeutic, or compensatory devices for injury or disability;
- examination, replacement, or modification devices for anatomy or physiological or pathological processes or conditions;
- devices for obtaining information through in vitro examination of samples from the human body, including organ, blood, and tissue donations. "

It is important to note that the MDC also covers accessories and custom-made medical devices, including software, which are commonly referred to as "active devices." The MDC also addresses the issue of market introduction (Chapter II), which places specific responsibility on manufacturers to ensure the safety of medical devices. This encompasses comprehensive quality management from production through to the end user. Manufacturers are required to label medical devices in accordance with instructions, communicate with the relevant authorities, implement risk management, monitor the placing on the market, and report and correct serious incidents. In accordance with the regulations, any violation is subject to legal penalties. The sale, commissioning, or other medical use of untested, unapproved, or harmful devices is generally prohibited. Medical devices are CE marked and accompanied by instructions for use in the language of the country in which the device is used. These instructions are clear and legible and provide detailed information on the device's intended uses, potential risks, and side effects. In the event that a product presents significant risks after it has been placed on the market, it must be withdrawn and may not be marketed until it has been made compliant. Furthermore, full traceability of all economic operators involved in the product must be ensured. It is also necessary to register all healthcare facilities and healthcare professionals to whom the product has been supplied in order to guarantee a seamless distribution chain. Furthermore, a UDI (Unique Device Identification System) must be assigned for unambiguous product identification and stored in a database (EUDAMED, European database for medical devices). Compliance with the regulations is monitored by a national authority in each MS.

Medical devices are classified into four risk categories, as follows: Class I (low risk), Class IIa (medium risk), Class IIb (higher risk), and Class III (highest risk) are the four categories used to determine the level of regulatory scrutiny. To illustrate, Class I devices, such as bandages and wheelchairs, permit manufacturers to self-certify compliance with General Safety and Performance Requirements (GSPR) without involving a notified body[534]. In contrast, Class IIa devices, such as hearing aids, necessitate a notified body's conformity assessment, clinical data for safety, and augmented post-market surveillance. Moreover, Class IIb devices, which include surgical lasers, are subject to a comprehensive assessment by a notified body, a detailed review of the clinical data, and rigorous monitoring. At the highest risk level, Class III devices, such as heart valves, are subject to the most rigorous notified body review, comprehensive quality management evaluation, and robust clinical trials, in addition to rigorous monitoring for adverse events.

The clinical evaluation of medical devices is crucial to EU regulatory compliance. By Article 61(1), this is intended to confirm compliance with the relevant essential safety and performance requirements when the device is used in a usual manner and in accordance with its intended purpose. This is done based on clinical data and a risk-benefit ratio analysis. A clinical evaluation is conducted in accordance with a clearly defined and methodologically sound process. This process includes, among other things, an evaluation of relevant literature, a critical analysis of the results of all available clinical studies, and consideration of alternative treatment options. It is important to note that clinical trials are subject to scientific and ethical review. Any conflicts of interest and potential non-compliance with EU law by the involved parties must be promptly identified and rectified.

It is important to note that responsibility for the safety of medical devices does not end after market launch. Once a device has been placed on the market, the EU regulation requires the implementation of additional continuous monitoring measures. This entails ongoing updates to the benefit-risk assessment, incorporating new data (and potential adverse events), clinical evaluation, revision of all device-related information, potential corrective actions, and the identification and reporting of trends. Manufacturers are required to submit an updated safety reports at least once a year, which must include data on total sales volumes and other relevant information. It is imperative that any severe incidents and safety corrective actions are taken in the field, or after establishing a causal link with the medical device, are documented and reported.

2. Clinical Trials Regulation

2.1. Scope

The Regulation on Clinical Trials on medicinal products for human use was issued on the 16th of April 2014 by the European Parliament and the Council. It applies to all clinical trials conducted in the European Union but does not apply to non-interventional studies. To ensure the safety of medical devices, manufacturers are required to conduct clinical trials in accordance with Regulation 536/2014 (see Chapters 1 and 2 of Regulation No. 536/2014). For close monitoring by the authorities, clinical trials must, therefore, also be preregistered and undergo a separate process before they are carried out (e.g.

[534] A notified body is an organization designated by an EU country to assess the conformity of certain products before being placed on the market (https://single-market-economy.ec.europa.eu/single-market/goods/building-blocks/notified-bodies_en)

approval by an ethics committee). On the one hand, this aims to maintain the quality of clinical studies at an exceptionally high level and, on the other hand, to ensure the safety of the participating individuals. As a result, according to the regulation, a clinical trial may be conducted *"only if (a) the rights, safety, dignity and well-being of subjects are protected and prevail over all other interests, and (b) it is designed to generate reliable and robust data."* (Article 3). Therefore, the regulation also contains, among other things, strict instructions on the pre-registration of a clinical trial as well as precise instructions on protocol, data protection, study design, reporting obligations or compensation for damages. Article 2(2)(1 and 2) of the Clinical Trials Regulation (Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on Clinical Trials on Medicinal Products for Human Use, and Repealing Directive 2001/20/EC Text with EEA Relevance, 2016) define what a clinical study and a clinical trial are:

- *A "clinical study" means any investigation about humans intended (a) to discover or verify the clinical, pharmacological or other pharmacodynamic effects of one or more medicinal products; (b) to identify any adverse reactions to tone or more medicinal products; or (c) to study the absorption, distribution, metabolism or excretion of one or more medicinal products; with the objective of ascertaining the safety and/or efficacy of those medicinal products.*
- *"Clinical trial" means a clinical study which fulfills any of the following conditions: (a) the assignment of the subject to a particular therapeutic strategy is decided in advance and does not fall within normal clinical practice of the MS concerned; (b) the decision to prescribe the investigational medicinal products is taken together with the decision to include the subject in the clinical study; or (c) diagnostic or monitoring procedures in addition to standard clinical practice are applied to the subjects.*

Usually, clinical trials are divided into different phases that serve various purposes (see Table 5 below). At the national level, the EU regulation is supplemented with regard to some points, with a view to national testing authorities. For example, in Germany DIN EN ISO 14155:2021-05 ("*Klinische Prüfung von Medizinprodukten an Menschen*") permits more extensive quality assurance measures (*DIN EN ISO 14155*, n.d.). Following good clinical practice guidelines, they are intended to provide performers with a gold standard. Furthermore, the DIN standard supplements the EU regulation to the effect that the use of a placebo is not possible for medical devices, and consequently, a significant (side) effect must be demonstrated by other methods.

Table 5. Clinical trial phases[535]

Phase	Dosing	Number of subjects	Main goal
0	Subtherapeutic	About 10	Pharmacokinetics and pharmacodynamics, microdosing
I	Ascending doses	20-100	Dose-ranging
II	Therapeutic dose	100-300	Drug efficacy
III	Therapeutic dose	1000-2000	Therapeutic effect
IV	Therapeutic dose	Anyone seeking treatment	Long-term effects
V	No dosing	All reported use	Research on data collected

[535] Mahan (2014).

In addition, there are several study design options utilized in the different trial phases (see Figure 1). For instance, randomized control studies are usually implemented in Phase III (Faller, 2019), whereas cohort studies are the method of choice in Phase IV. Finally, the results of the clinical trial, similar to those of pharmaceuticals, provide clear indications, contraindications, and instructions for the use of the respective medical device. Consequently, these medically used products contain instruction leaflets, can be further certified by the national testing authorities and finally (for example in Germany) be covered by health insurance companies.

2.2. Main provisions

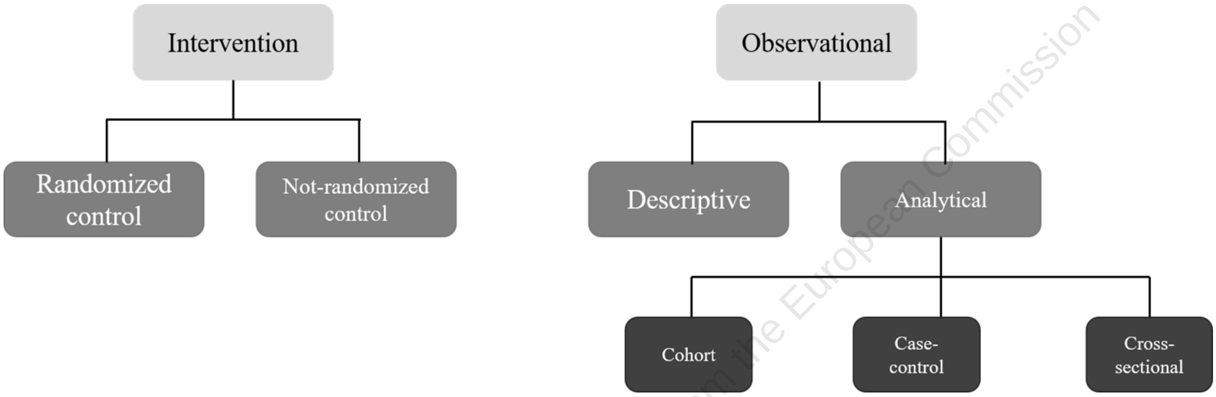

Figure 1. Overview on study designs (Kessler & Rothgangel, 2015)

The MDR mandates that manufacturers of medical devices furnish comprehensive documentation of all processes involved in the manufacture, distribution, and acceptance of such devices. Furthermore, a distinctive identifying number is allocated to each medical device, which can be accessed in a centralised and publicly accessible database (EUDAMED). Clinical trials are crucial to the medical device development process, particularly for higher-risk devices where safety and efficacy must be rigorously tested. In general, clinical trials are not required for Class I devices, as they pose a low risk. However, manufacturers must still provide evidence that the devices comply with the relevant regulatory standards. In the case of Class IIa devices, clinical trials may be required if there is insufficient clinical data available to demonstrate the safety and performance of the device. This is more common for devices that are either novel or possess new technological features. Class IIb devices frequently necessitate clinical trials to furnish substantial evidence of safety and efficacy, particularly for devices that profoundly impact patient health and involve elevated risks. Clinical trials are typically required for Class III devices due to their elevated risk and potential impact on patient health. These trials provide detailed data on the device's performance, safety, and potential side effects.

3. Applicability to XR

When employed for medical purposes, XR technologies are subject to the provisions of the MDR[536]. It is imperative that a risk classification be conducted initially. The risk classification of XR-based medical devices is dependent upon their intended use. However, it is not uncommon for manufacturers of XR-based medical devices, which are often software-based, to utilize XR technologies from other

[536] See for instance VR-therapy software for anxiety disorders by Sympatient GmbH Germany. EUDAMED DI: PP12332I.T.A.74 / IFA

manufacturers that have been developed for a different purpose. Consequently, MDR-compliant testing encompasses the software-based component, failing to cover any potential hardware malfunctions that may arise during operation. Clinical trials are highly structured experiments, the conduct of which is subject to a number of strict requirements. These requirements pertain to all aspects of the trial. Furthermore, there is an overlap with other regulations, such as those pertaining to data protection.

Nevertheless, concerns persist regarding the extent to which sensitive medical data collected using XR technology (e.g., virtual reality goggles) is adequately safeguarded. It is also noteworthy that many XR applications, such as those utilised for gaming or training, are not subjected to the same degree of rigorous examination. However, their use may have implications for medical practice. As the XR devices utilised were initially designed for recreational use, there is a notable deficiency in the hardware testing. It seems unlikely that manufacturers of medical products will also produce their own XR hardware due to the considerable costs associated with such development. If risks or side effects that pose a significant risk to the user become apparent during further use, the medical product may be subject to immediate recall. Individual addressing is made possible by the comprehensive documentation of the supply chain up to the end user.

11. Finance law

11.1. Anti-Money Laundering Directive

1. Overview of the Regulation

1.1. Scope

The Anti-Money Laundering Regulation (**AMLR**) is a new set of rules applicable to regulating the anti-money laundering domain. The AMLR arises from a series of EU Anti-Money Laundering Directives (**AMLDs**) which were aimed at preventing the misuse of the financial system for money laundering and terrorist financing The AMLR accordingly arose as a result of the adoption of the 6th AMLD and is part of the set of anti-money laundering rules that were adopted on the 30 May 2024 and that are now pending publication in European Official Journal before entering into force.[537]

The AMLR acknowledges the changing nature of money laundering and terrorist financing threats from outside the EU, facilitated by a constant evolution of technology and of the means at the disposal of criminals.[538] Accordingly, the inference is made that these developments require quick and continuous adaptations of the legal framework regarding third countries in order to address existing risks efficiently and prevent new ones from arising.[539]

The AMLR particularly acknowledges the continuous evolution of technology and the development of new products and systems for the exchange of funds or value.[540] The regulation proceeds to acknowledge that crypto-asset service providers and crowdfunding platforms are exposed to the misuse of new channels for the movement of illicit money and are well-placed to detect such movement and mitigate risks.[541]

In so doing, the Regulation highlights the need for Union legislation to be expanded to cover such entities, in line with the standards of the Financial Action Task Force about crypto-assets. While acknowledging advances in innovation, it is noted that the regulation explicitly acknowledges the development of the metaverse, which is likely to be used as a new avenue for the perpetration of crimes and for the laundering of their proceeds.[542] Drawing from this, the Regulation emphasises the need to exercise vigilance as regards the risks associated with the provision of innovative products or services, whether at the Union or national level or the level of obliged entities.[543]

The Regulation further acknowledges the need to extend the scope of the AML/CFT framework beyond the two types of crypto-asset service providers envisioned in the 5th AMLD which are providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers.[544] This need is emphasised upon by the rapid technological developments and the advancement in FATF

[537] Anti-money laundering: Council adopts package of rules (europa.eu)
[538] Recital 83, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Official Journal of the European Union
[539] Recital 83, Anti Money Laundering Directive
[540] Recital 7, Anti Money Laundering Directive
[541] Recital 7, Anti Money Laundering Directive
[542] Recital 7, Anti Money Laundering Directive
[543] Recital 7, Anti Money Laundering Directive
[544] Recital 14, Anti Money Laundering Directive

standards.[545] The Regulation acknowledges the ongoing evolution of relevant regulation to accommodate these technological developments through Regulation (EU) 2023/1114 (the MiCAR regulation), which has set requirements for crypto-asset service providers wishing to apply for an authorisation to provide their services in the internal market and further introduced a definition of crypto-assets and crypto-asset service providers encompassing a broader range of activities.[546]

The Regulation places the responsibility on the Anti Money Laundering Authority for the drawing up of regulatory technical standards on customer due diligence.[547] The standards are expected to set out the minimum information that is to be obtained by obliged entities to enter into new business relationships with customers or assess ongoing ones according to the level of risk associated with each customer.[548] Furthermore, the draft regulatory technical standards are required to provide sufficient clarity to allow market players to develop secure, accessible and innovative means of verifying customers' identity and performing customer due diligence while respecting the principle of technology neutrality.[549]

1.2. Subjects

The subjects encompassed under the regulation are the obliged entities previously highlighted and are listed in Article 3 of the Regulation. They include credit and financial institutions; legal and other professionals providing tax-related services or involved in financial or real estate transactions; trust or company service providers; estate agents and real estate professionals involved in high-value transactions; traders in precious metals, stones, and high-value goods; providers of gambling services; crowdfunding service providers and intermediaries; traders and intermediaries in cultural goods; credit intermediaries for mortgage and consumer credits; investment migration operators; non-financial mixed activity holding companies; football agents; and professional football clubs engaged in specific financial transactions.[550]

1.3. Main provisions

(a) **Business-wide risk assessment:** Article 10 of the AMLR provides that the obliged entities shall take appropriate measures that are proportionate to the nature of the business, including its risks, complexity and size, to identify and assess the risks of money laundering and terrorist financing to which they are exposed as well as the risks of non-implementation and evasion of targeted financial sanctions.[551] Specifically, the risk assessment is required to be carried out by businesses before the launch of new products, services or business practices, including the use of new delivery channels and new or developing technologies.[552]

(b) **Compliance functions:** Article 11 covers compliance functions under the regulation, requiring obliged entities to appoint a member of the management body in its management function to be responsible for ensuring compliance with the AMLR.[553] This compliance manager is required to

545 Recital 14, Anti Money Laundering Directive
546 Recital 14, Anti Money Laundering Directive
547 Recital 74, Anti Money Laundering Directive
548 Recital 74, Anti Money Laundering Directive
549 Recital 74, Anti Money Laundering Directive
550 Article 3, Anti Money Laundering Directive
551 Article 10(1), Anti Money Laundering Directive
552 Article 10(1), Anti Money Laundering Directive
553 Article 11(1), Anti Money Laundering Directive

ensure that the obliged entity's internal policies, procedures and controls are consistent with the obliged entity's risk exposure and that they are implemented.[554]

(c) **Group-wide requirements:** Under Article 16, a parent undertaking is required to perform a group-wide risk assessment, taking into account the business-wide risk assessment performed by all branches and subsidiaries of the group, and establish and implement group-wide policies, procedures and controls, including on data protection and on information sharing within the group for AML/CFT purposes as well as ensure that employees within the group are aware of the requirements arising from this regulation.[555] Further, the Regulation requires parent undertakings to implement those group-wide policies, procedures and controls, taking into account their specificities and the risks to which they are exposed.[556] In addition, Article 17 requires that where branches or subsidiaries of obliged entities are located in third countries and minimum compliance requirements are less strict than those set out in the AMLR, the parent undertaking shall ensure that those branches or subsidiaries comply with the requirements laid down in the regulation, including requirements concerning data protection, or equivalent.[557]

(d) **Customer due diligence:** Article 20 of the AMLR highlights the need to identify and verify a customer's identity as well as identifying the beneficial owners and taking reasonable measures to verify their identity so that the applicable regulatory entity is satisfied that it knows who the beneficial owner is and that it understands the ownership and control structure of the customer. Further obligations entail the assessment of the nature of business relationships and verifying whether the customer or the beneficial owners are subject to targeted financial sanctions. The obligations proceed to require entities falling within the scope of the Regulation to conduct ongoing monitoring of the business relationship, including the scrutiny of transactions undertaken throughout the business relationship, to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer.

(e) **Risks mitigation:** This aspect is covered in Article 40 of the Regulation, where crypto-asset providers are expressly referred to, and it is noted that the providers shall identify and assess the risk of money laundering and the financing of terrorism that is associated with transfers of crypto-assets directed to or originating from a self-hosted address. In this regard, the Regulation requires providers to have internal policies, procedures, and controls in place that allow for the implementation of mitigation measures commensurate with the risks identified. Providers are also required to constantly update these measures while considering latest technological developments.

2. Applicability to XR

2.1. Scope and subjects

The AMLR acknowledges the development of the metaverse and other XR technologies, acknowledging the risks arising out of the metaverse's existence on a decentralised platform without an existing and centralised architecture for supervision and regulation. This hinders compliance with traditional anti-money laundering requirements and results in the creation of potential new avenues for money

[554] Article 11(1), Anti Money Laundering Directive
[555] Article 16(1) , Anti Money Laundering Directive
[556] Article 16(1), Anti Money Laundering Directive
[557] Article 17(1), Anti Money Laundering Directive

laundering and terrorist financing.[558] It extends the scope of obliged entities to include crypto-asset service providers and crowdfunding platforms that are exposed to the misuse of XR for illicit money movement.

2.2. Obligations to XR providers

The AMLR establishes a comprehensive framework for regulating XR providers engaged in financial activities under the scope of the regulation to prevent their misuse for money laundering and terrorist financing. It extends AML obligations to new XR-related entities, requires risk assessments and due diligence tailored to XR, and emphasises data protection principles. Ongoing regulatory technical standards will further specify XR compliance requirements as the technology evolves. In particular, some of these obligations are the following:

(a) **Business-wide risk assessment:** XR providers would need to identify and assess the money laundering and terrorist financing risks that could arise from using new XR products, services, delivery channels and technologies before launching them. Ongoing risk assessments would be required as XR evolves.

(b) **Customer due diligence:** Acknowledging the decentralization of the metaverse, the AMLR increases the processes and relevant mechanisms that would apply to due diligence processes to counter the risks arising out of participant anonymity. Accordingly, XR providers must conduct thorough customer due diligence, including identifying and verifying customers and beneficial owners, assessing the purpose of transactions, and ongoing monitoring of XR-based business relationships. Regulatory technical standards will specify the minimum customer information required.

(c) **Risk mitigation:** The risks arising out of self-hosted addresses primarily arise from the multi-jurisdictional nature of transactions within the metaverse. This has accordingly resulted in the requirement through the regulation that sufficient transaction monitoring mechanisms are incorporated to monitor and maintain an up-to-date risk rating that allows for adequate profiling of customers and their financial behaviours. Crypto-asset service providers in XR would need to identify and assess the risks of transfers to/from self-hosted addresses and implement commensurate mitigation measures. These measures would need to be constantly updated as XR technology develops. Further, institutions are required to monitor the outbound and inbound movement of crypto assets recorded on-chain and the movements of crypto assets off-chain, paying particular attention to unusual transaction patterns or trans actions involving high-risk customers and locations.

(d) **Regulation of data collection and use:** While not directly addressed, the AMLR's emphasis on data minimisation, purpose limitation, and transparency in data processing would likely apply to the collection and use of personal data in XR environments. This is particularly applicable to the maintenance of transaction records for purposes of achieving accountability, facilitating audits, investigations and regulatory reporting. Compliance with the GDPR and other EU data protection laws would be required.

[558] "AML Compliance Challenges in the Metaverse." Sanction Scanner, www.sanctionscanner.com/blog/aml-compliance-challenges-in-the-metaverse-771. Accessed 6 Aug. 2024.

11.2. Electronic Money Directive

1. Overview of the Regulation

1.1. Scope

The Second Electronic Money Directive (**EMD2**), formally known as Directive 2009/110/EC, aims to establish a harmonised legal framework for issuing, pursuing the, and prudential supervision of electronic money institutions (**EMIs**) within the European Union. The EMD2 was published in the Official Journal of the European Union on 10 October 2009 and entered into force on 30 October 2009.[559] MS were required to transpose the directive into national law by 30 April 2011.[560]

The EMD2 sets out the rules on the business and supervision of EMIs to contribute to the emergence of a genuine single market for electronic money (or "**e-money**") services within the EU.[561] Further, this directive seeks to create a regulated category of an EMI with its own prudential and conduct regime.[562] This is tied to the proposals to introduce new requirements for the safeguarding and redeeming of customer funds and increase market stability by limiting exemptions to prudential requirements to small e- money institutions rather than all market participants for purposes of ensuring consistency with the Payment Services Directive in contributing towards a single European Market for payments for the benefit of consumers, business and the broader European economy.[563]

1.2. Subjects

The range of subjects is provided in Article 1 and is noted to encompass credit institutions and EMIs, which have been defined under the act as legal persons that have been granted authorisation under the Directive to issue e-money,[564] which in turn has been defined as any form of monetary value stored electronically and accepted as a means of payment.[565] This aligns with the Directive's objective of preparing a more straightforward and technology-neutral definition of e-money and removes the previous reference to defined storage mediums.[566]

The directive then proceeds to encompass post office giro institutions entitled under national law to issue e-money. The term "electronic money issuer" is defined to refer to the subjects of the Directive, as highlighted in Article 1(1). Notably, this definition also encompasses small e-money institutions, further building on the market stability objective, as aforementioned.[567].

[559] Article 24, EMD2
[560] Article 22, EMD2
[561] Electronic money: business and prudential supervision | EUR-Lex (europa.eu)
[562] Laying of regulations to implement the new E-Money Directive 1
[563] Electronic money: business and prudential supervision | EUR-Lex (europa.eu)
[564] Article 2(1), EMD2
[565] Article 2(2), EMD2
[566] Ruth Halpin, Roksana Moore, Developments in electronic money regulation – the Electronic Money Directive: A better deal for e-money issuers? Computer Law & Security Review, Volume 25, Issue 6, 2009, Pages 563-568
[567] Article 9, EMD2

1.3. Main provisions

(a) Issuance of e-money: Article 3 of the EMD2 outlines the requirements for the issuance of electronic money, providing that any natural or legal person who wishes to issue e-money must be authorised as an EMI and must comply with the other requirements of this directive.[568] This aligns with the market stability objective of the act by increasing regulatory control over the issuance of e-money. However, the Directive continues to exclude e-money issued for free, by retaining the requirement that, to fall within the scope of the legislation, e-money must be issued "on receipt of funds" and be accepted by a person "other than the e-money issuer."[569] Accordingly, this would exclude electronic money within XR virtual spaces where the money generated in the form of game tokens for instance would be excluded from the scope of this directive. In addition, the EMD2 establishes the following requirements to issue e-money:

i. **Initial capital requirements:** Article 4 of the directive sets out the initial capital requirements for EMIs, providing that these must hold an initial capital of at least €350,000 at the time of obtaining authorization to issue e-money.[570] The capital requirements serve as a consumer protection mechanism ensuring insulation of subscribers to issuers of electronic money from losses in the event of the issuers insolvency. Accordingly, this consumer protection objective continues to extend to the requirement that institutions hold at all times own funds that are at least equal to the sum of the requirements arising out of the different activities the issuer undertakes.[571]

ii. **Own funds requirements**: Article 5 of EMD2 sets out the ongoing capital requirements for EMIs, following the Capital Requirements Directive. EMIs must calculate their own funds using similar principles to those applied to banks and investment firms, and therefore ensures that EMIs maintain adequate financial resources throughout their operations, not just at the time of authorization. The calculation method for own funds is based on the institution's payment services activities and e-money issuance. This ongoing requirement complements the initial capital requirement and serves as an additional safeguard for consumer protection and market stability.

iii. **Business activities:** Article 6 of the EMD2 covers the business activities that e-money issuers are permitted to conduct while undertaking the business of electronic money issuance. Notably, the EMD2 relaxes the restrictions on issuers conducting business activities as the first Directive restricted issuers to engaging in business activities that are closely related to the lending and prevented the issuance of credit.[572] EMD2 allows EMIs to engage in the provision of payment services, granting of credit related to payment services, provision of operational services as well as closely related ancillary services in respect of the issuance of e-money or the provision of payment services as well as business activities other

[568] Article 3, EMD2
[569] Article 2(2), EMD2
[570] Article 4, EMD2
[571] Article 5(2), EMD2
[572] Ruth Halpin, Roksana Moore, Developments in electronic money regulation – the Electronic Money Directive: A better deal for e-money issuers? Computer Law & Security Review, Volume 25, Issue 6, 2009, Pages 563-568

than the issuance of e-money while having regard to applicable union and national legislation.[573]

iv. **Safeguarding requirements**: Article 7 establishes crucial safeguarding requirements for EMIs. The EMIs must protect customer funds received in exchange for issued e-money, aligning with the safeguarding methods outlined in the Payment Services Directive. This provision offers two primary options for safeguarding: either segregating customer funds from the institution's other assets and depositing them in a separate account with a credit institution or investing them in secure, liquid low-risk assets, or insuring the funds with an insurance company or credit institution. The core purpose of this article is to ensure consumer protection by safeguarding customer funds in the event of the EMI's insolvency, thereby maintaining trust in the electronic money system and promoting market stability.

(b) Exemption of requirements to issue e-money: The criteria against which a waiver can be granted by the relevant competent authority for purposes of requiring that an issuer be exempted from the compliance requirements listed in Articles 3, 4, 5 and 7 of the EMD2 are provided for in Article 9 which requires that the total outstanding e-money does not exceed €5,000,000[574] and further, that the persons responsible for the issuer have not been convicted of offences relating to money laundering, terrorist financing or other financial crimes.[575] These changes have reduced administration costs and may encourage more pilot schemes to appear as businesses and other organisations face fewer barriers to offering e-money services.

(c) Redemption requirements: Article 11 of EMD2 provides consumers the right to redeem e-money at par value at all times.[576] Article 11(4), however, incorporates a proviso for this right allowing issuers to charge a redemption fee that is commensurate to the actual costs incurred by the issuer if this fee is provided for in the contract between the e-money holder and the issuer. The fee shall be applicable in circumstances where redemption is requested before the termination of the contract, where the contract provides for a termination date and the e-money holder terminates the contract before that date, and lastly, where redemption is requested more than one year after termination of the contract.

2. Applicability to XR

EMD2 intersects with the proposed Markets in Crypto-Assets Regulation (MiCAR) regarding the regulation of e-money tokens, a crypto-asset referencing fiat currency. Issuers of e-money tokens may need to comply with both EMD2/PSD3 and MiCAR requirements. In summary, EMD2 provides a harmonised prudential framework for the issuance and regulation of e-money within the EU, aligning with the broader payments regulatory landscape. Its provisions aim to foster innovation while ensuring market stability and consumer protection, thereby presenting an opportunity for regulation to accommodate the impact of emerging technologies within financial markets.

[573] Article 6, EMD2
[574] Article 9(a), EMD2
[575] Article 9(b), EMD2
[576] Article 11(2), EMD2

This is particularly important within virtual worlds, noting that in the event that a metaverse is centralised where a central entity owns the rights to the platform and makes all final decisions, then the entity would make all decisions on how payments are effected in the platform.[577] In a centralized model the platform owner has full control over the payment system and can implement various protocols to manage the native token.

Taking for instance, Roblox, a user on the platform can purchase "Robux" -a virtual currency- in pre-defined packages at different prices, resulting in a variable exchange rate depending on the package size.[578] This allows Roblox to stabilise the value of "Robux" and establish clear pricing rules for the marketplace.[579] However, the centralized nature of the payment system can lead to barriers for users who wish to transact on other platforms and potential rent-seeking behaviour through payment fees and control over transaction data.[580]

The own funds requirements of Article 5 have significant implications for XR platforms operating as EMIs. These platforms must continuously maintain sufficient capital based on their e-money issuance and payment activities within virtual environments. This ongoing requirement could be challenging for smaller, innovative XR projects, potentially impacting their ability to scale or introduce new financial features in virtual worlds. However, it also enhances the financial stability of XR platforms, potentially increasing user trust in virtual economies. Applying these requirements to decentralised XR platforms, where there might not be a central entity responsible for maintaining capital reserves, could present unique regulatory challenges and may require innovative approaches to compliance.

Article 7 has significant implications for virtual world platforms and decentralised metaverse projects. XR platforms operating as EMIs must implement robust safeguarding measures for any in-game currencies or tokens that qualify as e-money under the directive. This could present unique challenges for decentralised XR platforms where there might not be a central entity responsible for fund management. The safeguarding requirements could potentially increase operational costs for XR platforms, which might impact smaller innovators in the space. However, these measures also enhance consumer protection in XR environments, potentially increasing user trust in virtual economies. For instance, platforms like Decentraland or The Sandbox VR would need to ensure that funds received for tokens like "MANA" or "SAND" are adequately safeguarded,[581] which could involve creating separate accounts for user funds or obtaining insurance. This requirement adds a layer of financial security to virtual transactions, potentially encouraging wider adoption of XR-based financial services while ensuring regulatory compliance in the evolving landscape of virtual economies.

[577] Cantú, Carlos, Cecilia Franco, and Jon Frost. "The Economic Implications of Services in the Metaverse." Global Perspectives in the Metaverse, edited by Hung-Yi Wu, Springer, 2024, pp. 123-145.
[578] Ibid.
[579] Ibid
[580] Ibid.
[581] In Decentraland there are particular tokens such as "MANA" (the ERC-20 token that allows users to claim parcels of "LAND" and trade with each other within the platform) and "LAND" (the ERC-721 token, associating each "LAND" parcel's x and y coordinates with a definition of a parcel's 3D scene that makes up the larger metaverse).

11.3. Markets in Crypto-Assets Regulation

1. Overview of the Regulation

1.1. Scope

The Markets in Crypto-Assets Regulation ("**MiCAR**") was first presented as a component of the European Commission's Fintech Action Plan. The MiCAR was published in the Official Journal of the European Union on 9 June 2023, effectively coming into force on 30 June 2023. The MiCAR rules concerning stablecoins (Titles III and IV) apply from 30 June 2024, while all MiCAR rules are expected to apply in full by 30 December 2024.

From the onset, the MiCAR recognised the need for the EU to develop legislative acts on financial services that are fit for the digital age and enable the use of innovative technologies. MiCAR then proceeds to highlight the EU's interest in developing and promoting the uptake of Distributed Ledger Technology (DLT) in the financial sector.[582]

The MiCAR then proceeds to highlight that crypto-assets, as one of the main applications of distributed ledger technology, are digital representations of value or rights that have the potential to bring significant benefits to market participants, including retail holders of crypto-assets.[583] This particularly applies to the uses and users of XR technologies noting that cryptocurrency-based incentives are used to reward creators for making contributions towards an XR ecosystem.[584] Accordingly, a legal framework for the protection of property rights arising from the allocation of crypto assets to users is needed.

MiCAR acknowledges that crypto-assets fall out of the scope of the EU's legislative acts on financial services, highlighting that it sets out to supplement the existing anti – money laundering regulations and legal framework.[585] Accordingly, the Regulation seeks to create legal certainty to facilitate the development of crypto-asset markets within the European Union, noting that the absence of rules for the regulation of crypto-assets creates room for holders of the assets to be exposed to risks that are not covered by consumer protection rules, thereby compromising market integrity in terms of market abuse as well as in terms of financial crime.

1.2. Subjects

MiCAR applies to any natural or legal persons and certain other undertakings that are engaging in the issuance, offer to the public and admission to trading of crypto assets, as well as the provision of certain services concerning crypto-assets within the EU. These services include:

- Custody and administration of crypto-assets on behalf of clients;
- Operation of a trading platform for crypto-assets;
- Exchange of crypto-assets for funds;
- Exchange of crypto-assets for other crypto-assets;
- Execution of orders for crypto-assets on behalf of clients;
- Placing of crypto-assets;
- Reception and transmission of orders for crypto-assets on behalf of clients;

[582] Recital 1, MiCAR
[583] Recital 2, MiCAR
[584] Role of Blockchain Technology in Extended Reality(XR)(lcx.com)
[585] Recital 4, MiCAR

- Providing advice on crypto-assets;
- Providing portfolio management on crypto-assets; and
- Providing transfer services for crypto-assets on behalf of clients.

MiCAR defines crypto-assets as a digital representation of value or rights that may be transferred and scored electronically using distributed ledger technology or similar technologies.[586] There is, however a proviso to this definition noting that the MiCAR does not apply to financial instruments and structured deposits falling within the scope of the Markets in Financial Instruments Directive, electronic money as defined in the E-Money Directive, except electronic money tokens under the same directive, deposits under the Deposit Guarantee Directive as well as securitisations as defined within the Securitization Regulation.[587]

Accordingly, the crypto-assets that fall within the domain of the Regulation include asset-referenced tokens (**ARTs**), money tokens (**EMTs**) and crypto-assets that are neither ARTs nor EMTs but do not fall within the exemptions as aforementioned. The MiCAR proceeds to define an asset-referenced token (ART) as a type of crypto-asset that is not an e-money token, and that purports to maintain a stable value by referencing another value or right or combination thereof.[588] The Regulation proceeds to define an e-money token as a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency.[589]

The key difference between e-money and e-money tokens lies in their technological underpinnings and regulatory classifications. E-money, as defined by the E-Money Directive, is electronically stored monetary value issued on receipt of funds and accepted as a means of payment by entities other than the issuer.[590] It does not necessarily utilise DLT. In contrast, EMTs are a subset of crypto-assets that use DLT and are designed to maintain a stable value by referencing a single fiat currency, such as the Euro or US Dollar. Consequently, while all e-money tokens are classified as e-money, not all e-money qualifies as e-money tokens unless they are crypto-assets utilising DLT.

The MiCAR proceeds to cover ARTs that are not financial instruments, stipulating authorisation requirements and obligations for issuers of these tokens under the Regulation. The offering of Asset-Referenced Tokens to the public and their admission to trading on a trading platform for crypto-assets require authorisation by the competent authority.

1.3. Main provisions

(a) Authorisation for ARTs issuers: The MiCAR stipulates that only legal entities with a registered office in the EU can be granted authorisation. MiCAR also requires issuers to publish a white paper, which must first be notified to the competent authorities as part of the application for authorisation. If authorisation is granted, the white paper is deemed to be

[586] Article 3(1) MiCAR
[587] Article 2(4) MiCAR
[588] Article 3(1) MiCAR
[589] Article 3(1) MiCAR
[590] Article 2(2), European Parliament and Council. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. Official Journal of the European Union, 10 Oct. 2009

approved.[591] Under Article 16, the issuance of ARTs is exempted from the authorisation requirement if:

i. over a period of 12 months, calculated at the end of each calendar day, the average outstanding amount of ARTs does not exceed EUR 5,000,000 or the equivalent amount in another currency;[592]
ii. the offer to the public of the ARTs is solely addressed to qualified investors, and the ARTs can only be held by such qualified investors.[593]

(b) Obligations for ARTs issuers:

- MiCAR provides for simplified requirements in the case of credit institutions within the meaning of point 28 of Article 3(1) of MiCAR.[594] Notwithstanding the exemptions from the authorisation requirement, issuers of ARTs must draw up a crypto asset white paper and notify this white paper to the competent authority of their home MS for approval.[595]
- MiCAR provides for several obligations and requirements for issuers of ARTs.[596] In addition to various obligations regarding communication with clients, publication, marketing communications, complaint handling, disclosure, governance and business organisation, MiCAR stipulates that issuers of ARTs must hold a sufficient level of own funds, create a recovery plan and a redemption plan and hold a reserve in the amount of their commitments arising from the issuance of tokens. In addition, the Regulation stipulates how the reserve assets are to be held in custody and invested.
- Where ARTs are classified as significant by the European Banking Authority (EBA) based on some of the criteria defined in Article 43 of MiCAR (size, volume, interconnectedness, etc.), issuers must fulfil additional obligations set out in Article 45 of MiCAR. In this case, the EBA becomes the supervisory authority responsible.

(c) Authorisation for EMTs issuers: Authorisation to issue EMTs is not granted to anyone or any company. No electronic money tokens are to be offered to the public in the EU or admitted to trading on a trading platform for crypto-assets unless the issuer of such EMTs.

i. is authorised as a credit institution or e-money institution and
ii. has notified a crypto asset white paper to the competent authority and published this crypto asset white paper in accordance with Article 51 of MiCAR.

It is thus not possible to apply for separate authorisation to issue EMTs; existing authorisation for credit institutions or e-money institutions constitutes the prerequisite for additionally issuing EMTs.

[591] Article 21(1) MiCAR
[592] Article 16 MiCAR
[593] Article 16 MiCAR
[594] Article 3(1) MiCAR
[595] Article 16(2) MiCAR
[596] Article 16 MiCAR

(d) **Obligations for EMTs issuers:** Since e-money tokens, as their name implies, are closely related to e-money, EMTs are explicitly to be regarded as e-money. In addition, EMT issuers are expected to comply with the provisions of the second E-Money Directive (EMD2) to a large extent, with only a few specific adjustments. Key aspects include the token holder's right to the reimbursement of the EMTs at par value at any moment and compliance with the security requirements under EMD2. Among the obligations set by the MiCAR are:

- Article 49 of MiCAR sets out provisions regarding the issuance and redeemability of EMTs. In detail, MiCAR grants the holders of EMTs a claim on the issuer of the respective EMTs. Moreover, MiCAR requires issuers to issue EMTs at par value on receipt of funds. EMT holders are entitled to request that an issuer redeem, at par value and at any moment, the monetary value of the EMTs. Neither EMT issuers nor crypto asset service providers are authorised to grant EMT holders interest or any other benefit during the period in which EMTs are held.[597] Furthermore, MiCAR covers questions concerning liability for white paper content and sets out rules regarding the investment of funds received in exchange for EMTs.

- Where the EBA classifies EMTs as significant based on some of the criteria defined in Article 56 of MiCAR (size, volume, interconnectedness, etc.), issuers must fulfil additional obligations (higher own funds requirements, requirements for holding reserve assets, etc.) set out in Article 58 of MiCAR. Where the issuer is an e-money institution, the responsibility for supervision is sometimes transferred to the EBA.

(e) **Other crypto-assets and special rules:** In contrast to the requirements for the issuance of ARTs and EMTs, the regulation does not provide an authorisation requirement for the issuance of other crypto-assets. To issue or offer to the public any type of crypto-assets (if no exemptions apply), issuers must notify a white paper to the competent authority and publish it, comply with requirements for marketing communications and grant token holders rights of withdrawal.[598] Moreover, issuers of crypto-assets other than ARTs or EMTs and persons seeking admission to trading for such crypto-assets must comply with conduct of business rules (Article 14 of MiCAR) and are to be held responsible for the information provided in a crypto asset white paper (Article 15 of MiCAR). The requirements above do not apply, for example, to issuers or providers of crypto-assets that are offered free of charge or where crypto-assets are issued as mining rewards.[599]

Under Article 59 of MiCAR, crypto asset services may generally only be provided by service providers with a registered office in the EU and have been authorised as crypto asset service providers by competent authorities by Article 63 of MiCAR. Under Article 60(1) to (6) of MiCAR, certain entities such as credit institutions, investment firms and e-money institutions can provide all or specific crypto asset services without separate authorisation. These entities must notify the competent supervisory authorities of their intention to take up business activities, providing the information stipulated in Article 60(7) of MiCAR.

[597] Article 50 MiCAR
[598] Article 6 et seq. MiCAR
[599] Article 4(3)(b) MiCAR

Funded by the European Union

2. Applicability to XR

2.1. Obligations

MiCAR's applicability to the regulation and governance of the metaverse and XR technologies can be drawn from its applicability to the regulation of cryptocurrencies, tokens, and other thematic areas, as highlighted below.

(a) Digital currencies and NFTs in the metaverse

- **Crypto tokens and NFTs**: The metaverse often employs cryptocurrencies and non-fungible tokens (NFTs) for transactions and ownership of digital assets. MiCAR's provisions on the issuance and trading of crypto-assets, including transparency and disclosure requirements, directly apply to these digital currencies and NFTs.
- **Marketplaces and trading platforms**: MiCAR regulates the operation of trading platforms for crypto-assets, which are essential for buying and selling digital assets within the metaverse. This includes ensuring the integrity of these platforms and protecting users from market abuse.

(b) Consumer protection and financial stability

- **User protection**: As users engage in financial transactions within the metaverse, MiCAR's consumer protection measures, such as the requirement for white papers and marketing communications, safeguard users from potential fraud and financial crimes.
- **Systemic Risk Management**: The regulation of significant asset-referenced tokens (ARTs) and electronic money tokens (EMTs) under MiCAR aims to mitigate systemic risks that could arise from their widespread adoption in the metaverse.

(c) Innovation and fair competition

- **Supporting innovation**: MiCAR encourages innovation by providing a secure regulatory environment for new technologies. This is crucial for developing decentralized applications and financial services within the metaverse.
- **Interoperability and portability**: The regulation also addresses issues related to the interoperability and portability of digital assets, which are vital for the seamless functioning of the metaverse across different platforms and applications.

2.2. Challenges

- **Decentralized Finance (DeFi)**: MiCAR explicitly excludes fully decentralised finance and native cryptocurrencies like Bitcoin from its scope. This exclusion poses challenges for regulating decentralised applications within the metaverse that rely on these technologies.
- **Jurisdictional issues**: The global nature of the metaverse complicates the enforcement of MiCAR, as it can be challenging to identify the jurisdiction of service providers operating in a decentralised environment.
- **Data security and privacy**: The metaverse raises significant concerns about data security and privacy, which are not fully addressed by MiCAR. Regulations like the

General Data Protection Regulation (GDPR) must work in tandem with MiCAR to ensure comprehensive protection.

Funded by the European Union

11.4. Regulation for the Digital Operational Resilience for the Financial Sector

1. Overview of the Regulation

1.1. Scope

The Regulation 2022/2554 on digital operational resilience for the financial sector (known as **Digital Operational Resilience Act** or **DORA**) is a regulation which aims to ensure that all financial firms have better control of ICT risks making them more resilient to cyber threats and ICT disruptions. DORA was first proposed by the European Commission in September 2020 and is part of a larger digital financial package that includes initiatives for regulating crypto-assets and enhancing the EU's overall digital finance strategy. The Council of the European Union and the European Parliament (the legislative bodies responsible for approving EU laws) formally adopted the DORA in November 2022. Financial entities and third-party ICT service providers have until 17 January 2025 to comply with DORA before enforcement starts.[600]

While the EU has officially adopted DORA, critical details are still being ironed out by the European Supervisory Authorities (**ESAs**). The ESAs are the regulators that oversee the EU financial system, including The European Banking Authority (EBA), the European Securities and Markets Authority, and the European Insurance and Occupational Pensions Authority. The ESAs are in charge of drafting the regulatory technical standards (RTS) and implementing technical standards (ITS) that covered entities must implement.[601]

The scope of DORA is noted in Article 2 and includes all supervised financial entities, not only traditional financial entities such as banks, insurance and investment firms.[602] DORA also applies to less traditional financial entities, such as credit rating agencies, trade repositories, payment and e-money institutions, and trading venues.[603] DORA also applies to crypto-asset service providers as authorised under MiCAR and issuers of asset-referenced tokens.[604]

Further, the scope of DORA includes all financial entities regardless of their criticality for the financial sector making it a law of special application (*lex specialis*) encompassing legal principles on cyber resilience for all financial firms. DORA therefore takes precedence over the more general cybersecurity rules laid down in the NIS2 Directive in situations where they overlap.

DORA is crucial because it focuses on making financial systems resilient to disruptions caused by digital advancements.[605] This highlights the EU's commitment to a stable and reliable financial landscape as the world becomes more digital.[606] By setting strict rules for managing digital operations, DORA acknowledges the growing danger of cyber threats and emphasises the need for a unified EU response.[607]

---

[600] IBM, [What Is the Digital Operational Resilience Act (DORA)?]()
[601] Ibid.
[602] Clausmeier, D. Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *Int. Cybersecur. Law Rev.* **4**, 79–90 (2023). https://doi.org/10.1365/s43439-022-00076-5
[603] Ibid.
[604] Ibid.
[605] [Grand Compliance - Blog - DORA Regulation: Bafin Digital Operational Resilience Act]()
[606] Ibid.
[607] Ibid.

Accordingly, this regulation establishes a harmonised framework for the management of information and communication technology (ICT) risks, ensuring the resilience and security of financial services across the EU.

1.2. Subjects

The range of subjects is provided for in Article 2, and they include electronic money institutions, crypto-asset service providers and issuers of asset-referenced tokens, trading venues, trade repositories, crowdfunding service providers and ICT third-party service providers such as cloud computing service providers, among others. The Act refers to all the foregoing parties as "financial entities".[608]

1.3. Main provisions

DORA introduces several key provisions to enhance digital operational resilience within the financial sector. To start with, the Regulation defines digital operational resilience as the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring either directly or indirectly, through the use of services provided by ICT third-party service providers, the full range of ICT related capabilities needed to address the security of the network and information systems that a financial entity uses and which support the continued provision of financial services and their quality, including throughout disruptions.[609]

The DORA goes on to define ICT concentration risk as an exposure to an individual or multiple related critical ICT third-party service providers, creating a degree of dependency on such providers so that the unavailability, failure or other types of shortfall of such providers may potentially endanger the ability of a financial entity to deliver critical or important functions or cause it to suffer other types of adverse effects such as significant losses, or endanger financial stability.[610]

Article 4 introduces the proportionality principle, which provides that financial entities shall implement rules by the principle of proportionality while taking into consideration their size as well as overall risk profile together with the nature, scale and complexity of their services, activities and operations.[611] When considering the application of the proportionality principle, regulatory authorities are required to consider the application of the proportionality principle by reviewing the consistency of the ICT risk management framework based on the reports submitted by the different financial entities.[612]

Article 5 introduces the requirement that financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk in order to achieve a high level of digital operational resilience.[613]

The respective entities are required to have a management body that shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework.[614] This body is required to bear the ultimate responsibility fort managing the financial entity's

[608] Article 2, DORA
[609] Article 3(1), DORA
[610] Article 3(29), DORA
[611] Article 4(1), DORA
[612] Article 4(3), DORA
[613] Article 5(1), DORA
[614] Article 5(2), DORA

ICT risk and put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity as well as confidentiality of data.[615]

These management bodies are also required to ensure effective and timely communication, cooperation and coordination by setting up appropriate governance arrangements, determining the appropriate risk tolerance level of ICT risk, review, implementation of the financial entity's ICT business continuity policy together with its response and recovery plans.[616] Further, the management body will be required to put in place reporting channels enabling it to be duly informed of arrangements that have been concluded with third-party ICT service providers on the use of ICT services together with any relevant planned material changes regarding ICT third-party service providers.[617]

Article 6 of the DORA covers the ICT risk management framework. Here it is posited that the ICT framework shall be sound, comprehensive and well documented, enabling them to address ICT risk quickly, efficiently as well and comprehensively for purposes of ensuring a high level of digital operational resilience.[618] Further, the framework is required to include strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, and servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage.[619]

Article 7 requires financial entities to use and maintain updated ICT systems, protocols and tools that are appropriate for the magnitude of operations supporting the conduct of their activities in accordance with the proportionality principle.[620] Further, the systems are required to be reliable and equipped with a sufficient capacity to process the data necessary for the performance of activities as well as the timely provision of services while dealing with peak orders, messages or transaction volumes as needed, including where new technology is introduced.[621]

Article 8 discusses the ICT risk management framework and requires financial entities to identify, classify and adequately document all ICT-supported business functions, roles and responsibilities together with all information assets and ICT assets supporting those functions as well as their roles and dependencies about ICT risk.[622] In addition, financial entities are required to identify and assess all sources of ICT risk and, in particular, the risk exposure to and from other financial entities.[623] This includes taking stock of all information assets and ICT assets, including those on remote sites, network resources, legacy systems, and hardware equipment, while mapping those considered critical.[624]

Article 10 requires financial entities to have in place mechanisms to promptly detect anomalous activities.[625] This requires entities to put in place a comprehensive ICT Business Continuity Policy, which will ensure the restoration of systems and data with minimum downtime and limited disruption and

[615] Article 5(2)(b), DORA
[616] Article 5(2)(d), DORA
[617] Article 5(2)(i)(ii), DORA
[618] Article 6(1), DORA
[619] Article 6(2), DORA
[620] Article 7(c) , DORA
[621] Article 7(c) , DORA
[622] Article 8(1) , DORA
[623] Article 8(2) , DORA
[624] Article 8(3) , DORA
[625] Article 10(1) , DORA

loss.[626] Further, as part of their ICT risk management framework, financial entities shall develop and document backup policies and recovery methods together with a communication strategy.[627]

In summary, DORA seeks to cover four main pillars of operational resilience for financial entities. It covers the cybersecurity requirements arising out of the reporting of ICT related incidents and notifications, digital operational resilience testing, as well as information and intelligence sharing. Further, it covers the requirements related to the contractual agreements between ICT third-party service providers and financial institutions. This is noted in Article 28 of the Regulation, which provides that these contractual provisions will be required to include provisions on accessibility, availability, and integrity, as well as provisions on ensuring access, recovery, service level descriptions and right of termination and the obligation of the third-party service provider to help in the event of an ICT related incident.[628]

2. Applicability to XR

2.1. Subjects regulated within the XR ecosystem

DORA's provisions primarily focus on the financial sector, including entities such as credit institutions, payment institutions, investment firms, and insurance companies. However, the regulation may have implications for XR providers that offer services to these financial entities or are considered critical ICT third-party service providers.

In understanding the applicability of DORA and its implications for financial entities, understanding the relevance of platforms like Roblox is crucial. Roblox's Developer Exchange program allows users to convert Robux, the platform's virtual currency, into fiat currency.[629] This feature effectively positions Roblox as a financial entity for regulatory purposes, necessitating compliance with operational resilience standards to ensure uninterrupted service provision. DORA aims to strengthen the IT security and operational resilience of financial entities and their critical third-party service providers, including those offering digital and data services. Platforms like Roblox, which facilitate financial transactions through virtual currencies, must adhere to DORA's stringent requirements to manage ICT risk effectively. This includes undergoing audits, adhering to security standards, and potentially facing direct oversight by European Supervisory Authorities. The regulation ensures that financial entities, and by extension platforms like Roblox, maintain robust systems to prevent disruptions that could compromise service provision to users.

2.2. Obligations for XR providers

If an XR provider is classified as a critical ICT third-party service provider under DORA, it would be subject to the oversight framework established by the regulation. This could entail adhering to specific security and resilience standards, undergoing audits, and potentially facing direct oversight by the European Supervisory Authorities. Additionally, XR providers that offer services to financial entities regulated under DORA may be required to comply with the third-party risk management provisions outlined in the regulation. Financial entities must ensure that these XR providers meet the security and resilience requirements.

[626] Article 11(1) , DORA
[627] Article 12(1) , DORA
[628] Article 28(3), DORA
[629] Earned Robux, Earned Robux Wallet and DevEx Rates – Roblox Support

Funded by the European Union

For example, BearingPoint, a prominent provider of XR consulting services and platforms, is one such XR provider that could be applicable in this context. BearingPoint offers comprehensive XR solutions, including strategy development, business integration, application development, and ongoing support, ensuring that their services align with regulatory standards and help financial entities manage third-party risks effectively.[630] BearingPoint's expertise in integrating XR solutions into business processes and providing long-term support and service level agreements (SLAs) positions them as a critical ICT provider that must adhere to DORA's stringent requirements to ensure operational resilience and security for financial entities.[631]

2.3. Challenges

One potential challenge in implementing DORA within the XR ecosystem is the rapidly evolving nature of XR technologies and their applications. The regulation may need to be regularly updated or supplemented with additional guidance to address the unique risks and challenges posed by XR technologies in the financial sector.

Furthermore, the existing regulatory framework may have gaps regarding the specific treatment of XR technologies and their integration with financial services. As XR adoption continues to grow, additional regulatory efforts may be required to ensure that these technologies are adequately covered under the digital operational resilience framework established by DORA.

It is important to note that the analysis is based on the information available in the provided search results and the explicit provisions quoted from the regulation. As DORA is a relatively new regulation, its practical implementation and potential impact on the XR ecosystem may evolve, requiring further assessment and adaptation.

[630] Extended Reality (XR) Services." BearingPoint, www.bearingpoint.com/en-nl/services/technology/xr-services/. Accessed 6 Aug. 2024.
[631] Ibid.

Funded by the European Union

12. Conclusions

In this report, we have analysed 25 pieces of EU legislation (regulations and directives) and one international treaty. These have different levels of applicability to the use, development, and offer of XR technologies.

The pieces of regulation that are generally applicable to all XR providers are the General Data Protection Regulation (GDPR), the Data Act, the Trademark Regulation, the Consumer Rights Directive (CRD), the Unfair Commercial Practices Directive (UCPD) and the European Accessibility Act. Some providers may be also subject to the NIS2 Directive when deployed by entities that are part of critical sectors (e.g. healthcare) and the Trade Secrets Directive (TSD).

Several of the former regulations embed the classification between products (or goods) and services to define the obligations to manufacturers, traders or sellers. This classification is relevant for the XR environment, as providers of XR hardware (i.e. headsets and haptic XR) or non-online XR software will be regulated as product manufacturers, while providers of XR online services and platforms will be regulated as service providers.

The former classification is also relevant for the definition of additional pieces of regulation that target each of those categories:

- Manufacturers of XR hardware are also obliged by the Product Safety Regulation, and in some cases, they may be subject to the Medical Devices Regulation.
- Providers of XR services are also obliged by the Copyright in the DSM Directive, the Digital Content Directive (DCD), the obligations for online platforms in the Digital Services Act (DSA), and the Child Sexual Abuse Regulation. These providers will be under additional law depending on particular conditions established by them:
    - If the XR service is recognised as an electronic communications service, the e-Privacy Directive is applicable.
    - If the provider is recognised as a data intermediary, the Data Governance Act (DGA) is applicable.
    - If the provider is recognised as a media service provider, the Audiovisual Medial Service Directive (AVMSD) is applicable.
    - If the XR service is designated as core platform services provided by a gatekeeper, the Digital Markets Act (DMA) is applicable.
    - If the XR service is used in the public sector, the Web Accessibility Directive (WAD) is applicable.
    - The AI Act applies if the XR provider is providing or deploying an AI system.
    - If the XR provider engages in financial activities, the Anti-Money Laundering Directive (AMLD) and the Regulation for the Digital Operational Resilience for the Financial Sector (DORA) may be applicable.
    - If the XR provider issues crypto-assets, the Markets in Crypto-Assets Regulation and/or the E-Money Directive may be applicable.

Several of these regulations may be applicable in parallel to an XR provider regarding a specific topic. For example, when XR users are shown deals in a virtual space on their favourite products in real-time based on his/her previous behaviour. The GDPR will have an important role in processing personal data, with Article 6 requiring a lawful basis and Article 7 detailing the conditions for valid consent. In addition, Article 21 of the GDPR allows individuals to object to their data being used for direct marketing. The e-Privacy Directive may also have a role, given that Article 5(3) mandates the XR provider to obtain consent before using tracking technologies, like cookies, to monitor user behaviour for marketing purposes in the Metaverse (i.e. opt-in instead of opt-out). Article 5 of the UCPD prohibits the XR provider's misleading and aggressive marketing tactics, while Article 11a ensures consumers harmed by such practices have access to remedies. The CRD, with particular reference to Article 6, requires clear and comprehensive information about products and services to ensure sustained transparency in VR marketing.

The analysis in this report reveals a multi-faceted regulatory framework impacting entities in the European and global XR sectors vis-à-vis providing XR products or services to the European market. The foregoing analysis has aimed to focus on the salient points of relevant regulatory frameworks and highlights their potential or current role in mitigating risks posed by XR technology. XR technology, in certain aspects, promises to introduce novel concerns, while in other aspects, we note newer dimensions of existing issues. For example, novel risks due to XR technology, such as virtual sexual assault require expanding the current notion of 'cybercrimes'. On the other hand, the additional processing of biometric personal data, the potential of identity theft online or the role of data inequality in this sector highlight the relevance of technology-neutral laws that can accommodate these newer dimensions of normatively understood concerns.

While existing legislation and regulations continue to be amended to counter emerging dynamics and the changing environment, it is unlikely that the amendments will keep pace with the development and uptake of XR technologies. As with many new and emerging technologies, the pace of technological development is much faster than that of regulatory coverage of the issues they bring up to the forefront. There is a need to foster adaptable regulations that can be readily updated to catch up with the development of XR technologies. This report allowed us to identify the relevant regulations that one should concentrate upon and the challenges (or gaps) that must be addressed. The next step is to develop a policy roadmap that will suit this purpose. Based on the description of the state-of-art in the policy debates (Deliverable D3.1) and the current regulatory gap analysis (Deliverable D3.2), the final Deliverable (D3.3) will provide the answers on necessary policy and regulatory steps to ensure a comprehensive human-centred, socially sustainable, ethical and commercially successful XR technology development.