



C O R T E X ²

D4.2 – In-depth analysis and guidelines



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement n° 101070192. This document reflects only the author's view, and the EU Commission is not responsible for any use that may be made of the information it contains.



D4.2 – In-depth analysis and guidelines

Project Title	COoperative Real-Time EXperiences with EXtended reality
Project Acronym	CORTEX ²
Grant Agreement No	101070192
Instrument	HORIZON Innovation Actions
Topic	HORIZON-CL4-2021-HUMAN-01-25
Start Date of Project	September 1, 2022
Duration of Project	36 months

Name of the Deliverable	In-depth analysis and guidelines
Number of the Deliverable	D4.2
Related WP Number and Name	WP4
Related Task Number and Name	T4.2
Deliverable Dissemination Level	
Deliverable Due Date	September 2024
Deliverable Submission Date	30 August 2024
Task Leader/Main Author(s)	CiTIP - KU LEVEN Franklyn Ohai Dr Maja Nisevic



	Prof Jan De Bruyne
Contributing Partners	Azucena Garcia Palacios (Universitat Jaume I De Castellon (UJI)) Alain Pagani (Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI))
Reviewer(s)	

Keywords

GDPR, data governance, natural language processing, extended reality, mix reality, virtual reality, augmented reality, artificial intelligence, generative AI, virtual assistants, teleconferencing, remote work.

Revisions

Version	Submission date	Comments	Author
v0.1	24/06/2024	Initial draft	Franklyn Ohai
v0.2	28/06/2024	Feedback	Maja Nisevic
V0.3	30/06/2024	Revision	Franklyn Ohai



Disclaimer

This document is provided with no warranties whatsoever, including any warranty of merchantability, non-infringement, fitness for any particular purpose, or any other warranty with respect to any information, result, proposal, specification or sample contained or referred to herein. Any liability, including liability for infringement of any proprietary rights, regarding the use of this document or any information contained herein is disclaimed. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by or in connection with this document. This document is subject to change without notice. Reincarnate has been financed with support from the European Commission. This document reflects only the view of the author(s) and the European Commission cannot be held responsible for any use which may be made of the information contained.



Acronyms and definitions

Acronym	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
B2B	Business-to-Business
B2G	Business-to-Government
CRA	Cyber Resilience Act
CSA	Cyber Security Act
DMA	Digital Markets Act
DPIA	Data Protection Impact Assessment
DSA	Digital Services Act
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
EU	European Union
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
GPAI	General Purpose AI
HLEG	High-Level Expert Group
IoT	Internet of Things
MR	Mixed Reality
NIS2	Network and Information Security 2
NLP	Natural Language Processing
SaaS	Software as a Service
SDK	Software Development Kit
VR	Virtual Reality
XR	Extended Reality



Contents

1. Introduction	9
1.1. Structure of the document.....	10
2. Ethics in CORTEX ²	10
2.1. Ethics in AI.....	11
2.1.1. High-Level Expert Group (HLEG) Guidelines for Trustworthy AI.....	11
2.1.2. Respect for human autonomy.....	12
2.1.3. The principle of harm prevention	14
2.1.4. Principle of fairness:.....	14
2.1.5. Principle of explicability	14
2.2. Requirements for Trustworthy AI	15
2.3. Ethics in XR	20
3. Privacy and data protection	22
3.1. Data Protection Principles.....	23
3.1.1. Lawfulness Fairness and Transparency.....	24
3.1.2. Purpose Limitation	24
3.1.3. Data minimisation principle.....	25
3.1.4. Accuracy Principle.....	26
3.1.5. Storage Limitation Principle.....	27
3.1.6. Integrity and Confidentiality	28
3.2. Data Subject Rights	28
3.2.1. Right to be Informed	29
3.2.2. Right of Access	31
3.2.3. Right to rectification	32



3.2.4.	Right to Erasure (right to be forgotten)	33
3.2.5.	Right to restrict processing	33
3.2.6.	Right to object	34
3.2.7.	Right to withdraw consent	34
3.2.8.	Right to Data Portability	35
3.2.9.	Right to object to automated individual decision-making	35
3.2.10.	Right to lodge complaints with a supervisory authority	35
3.3.	Additional requirements under the GDPR	36
3.4.	Relevant GDPR Roles	37
4.	Analysis of the AI ACT	39
4.1.	Relevant Actors Pursuant to AI Act	39
4.2.	Salient Observations on AI Act trajectory:	40
4.3.	Legal Certainty for General Purpose AI	41
4.4.	Requirement to Implement AI Literacy	42
4.5.	Transparency Requirements	43
5.	Cybersecurity framework for CORTEX ²	45
5.1.	Cybersecurity Concerns Specific to XR Technologies	46
5.2.	Cyber Security Act	46
5.2.1.	Objectives and Importance of the CSA	47
5.2.2.	Obligations of Manufacturers	48
5.2.3.	Certification Schemes	49
5.3.	NIS2 Directive	50
5.4.	Overview of Cyber Resilience Act Proposal	51
5.4.1.	Applicability of CRA to CORTEX ²	52



5.4.2.	Exclusions for Open-Source and Non-Commercial Software	53
6.	Data Governance Framework	54
6.1.	The EU Data Act.....	55
6.2.	Digital Services package	56
6.2.1.	Digital Services Act.....	57
6.2.2.	Digital Markets Act.....	58
7.	Conclusion	60

1. Introduction

Deliverable D4.2 is part of Work Package 4 of the CORTEX2 project. This document marks the completion of Task T4.2, which involves a comprehensive legal and ethical analysis of the CORTEX² project. Task T4.2 is scheduled for completion in Month 24 of the project. The purpose of this report is to provide clear guidance to the consortium and inform stakeholders about the legal and ethical considerations relevant to CORTEX2.

This deliverable builds on the preliminary analysis presented in Deliverable D4.1, submitted in Month 13. Section 2 of Deliverable D4.1 identified and analysed the initial ethical requirements for CORTEX2, focusing on its main features and enabling technologies, while Sections 3 -5 deal with the preliminary legal requirements based on EU legal framework. In this deliverable, we delve deeper into the ethical requirements for CORTEX2, particularly the main components such as avatar generation, speech technology, natural language processing, scene semantics, and IoT integration. We also revisit the key regulatory areas identified in the initial tasks, including privacy and data protection, AI component regulation, cybersecurity, data governance, and market considerations.

In analysing the main components of CORTEX2 (avatar generation, speech technology and natural language processing NLP, scene semantics and 3D scene reconstruction, IoT integration and conversational agents) this deliverable establishes that privacy, data protection principles, and the protection of the rights of data subjects, as envisaged in the GDPR are of paramount importance.¹ As part of the analysis, it is essential to evaluate the roles of various actors in CORTEX², specifically identifying the controller, joint controller, or processor in the relevant contexts. Additionally, it is crucial to identify the relevant actors developing, deploying, or otherwise making available General Purpose AI models or systems as envisaged in the AI Act.² Developers, deployers, or other parties identified in the AI Act must comply with the relevant

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1

² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 173/1.



obligations, especially, given the intention to deploy CORTEX² solutions for remote work and learning.

Moreover, numerous cybersecurity issues are associated with XR in the context of remote work, and this deliverable aims to analyse these issues and identify potential solutions based on the EU regulatory framework. Additionally, the variety of device interfaces in CORTEX² enables new methods of data collection, which can yield insights about users, bystanders, and performance data from businesses. Therefore, it is crucial to develop a comprehensive roadmap for data governance to address these challenges effectively.

The guidelines developed in this deliverable will form the basis for the validation and recommendations developed in Task T4.3 and published in Deliverable D4.3.

1.1. Structure of the document

The next section of this deliverable, Section 2, provides an in-depth analysis of the ethical requirements for CORTEX². Section 3 elaborates the legal requirements for CORTEX² based on the introductory part of this report, focusing on privacy and data protection and the regulatory tracks identified in section 3 to 5 of Deliverable D4.1. Section 4 addresses the AI Act and how it applies to CORTEX². Section 5 is an in-depth analysis of the cyber security framework, while Section 6 is a deeper exploration of data governance and market considerations.

2. Ethics in CORTEX²

Ethics plays a crucial role in the design, development, and deployment of XR technologies like CORTEX². This importance stems from the foundational technologies of XR, such as AI, and their intended applications across various sectors, including remote work, healthcare, emergency services, entertainment, and education.³ The advent of these complex technologies necessitates an urgent examination of their ethical and social implications. The decisions made regarding the development, adoption, and use of these technologies will significantly impact future lives.⁴ Therefore, a proactive approach to identifying and addressing ethical concerns is

³ 'EU Funding & Tenders Portal' <<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/competitive-calls-cs/4061>> accessed 28 June 2024

⁴ James H Moor, 'Why We Need Better Ethics for Emerging Technologies' (2005) 7 Ethics and Information Technology 111



vital to fostering trust and promoting the beneficial use of XR technologies in society. To this end, this deliverable identifies a two-pronged ethical challenge: ethics in AI and ethics in XR.⁵

2.1. Ethics in AI

Ethics in AI is relevant address significant ethical issues, such as fairness, bias, accountability, and transparency.⁶ AI systems can inadvertently perpetuate and even exacerbate existing biases, complicating the assignment of responsibility for their actions. Therefore, appropriate ethical frameworks and assessment tools are needed to address these issues and ensure that AI development and deployment adhere to ethical principles such as non-maleficence. To this end, this deliverable takes a deeper look at the HLEG ethics guidelines for trustworthy AI to evaluate how the CORTEX² AI components measure up against the ethical principles of (1) respect for autonomy, (2) prevention of harm, (3) fairness, and (4) explicability.⁷

Ethics in XR is crucial in the design, development, and deployment of XR solutions.⁸ As previously noted in Deliverable D4.1,⁹ accessibility and human autonomy are significant issues in XR. Additionally, introducing such technologies into the workplace can perpetuate existing biases or create new ones. Therefore, it is essential to ensure that ethical requirements, such as those identified by the HLEG, are considered throughout the lifecycle of CORTEX².

2.1.1. **High-Level Expert Group (HLEG) Guidelines for Trustworthy AI**

Governments and policymakers worldwide have begun to identify the critical issues posed by AI and are not only developing national strategies to enhance AI but also assessing its risks and determining effective policies to mitigate them.¹⁰ Launching the AI HLEG was part of the EU's strategy to address these challenges, particularly given the rapid advancement of AI in the absence of a normative regulatory framework within the EU. Although the absence of specific

⁵ Koroglu, Osman. "Ethics in AI, XR and Digitalization: A Systematic Literature Review." In BOOK OF PROCEEDINGS, p. 109.

⁶ *ibid.*

⁷ High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (2019) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 accessed 28 June 2024.

⁸ *ibid*; Melvin Abraham and others, 'Implications of XR on Privacy, Security and Behaviour: Insights from Experts', Nordic Human-Computer Interaction Conference (Association for Computing Machinery 2022) <<https://dl.acm.org/doi/10.1145/3546155.3546691>> accessed 2 June 2024.

⁹ Deliverable D4.1 Ethical and Legal Inventory, p.23.

¹⁰ Nathalie A Smuha, 'The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence' (2019) <<https://papers.ssrn.com/abstract=3443537>> accessed 2 June 2024.



laws is now being gradually addressed by the adoption of the Artificial Intelligence Act, the ethical imperatives from the HLEG Guidelines for Trustworthy AI remain relevant. These guidelines attempt to operationalise ethical principles in socio-technical systems.¹¹ As noted in the HLEG Guidelines, AI systems should be developed, deployed, and used in ways that adhere to the ethical principles of respect for human autonomy, prevention of harm, fairness, and explicability. To achieve these principles, the HLEG has set out seven requirements for trustworthy AI. However, before discussing these requirements and their relevance for CORTEX2, it is essential to understand the objectives of these principles, especially in light of using AI-powered solutions for remote work, learning and other socio-economic endeavours.

2.1.2. Respect for human autonomy

The principle of respect for human autonomy aims to ensure that individuals interacting with AI systems retain their free will and can participate in democratic processes.¹² This principle seeks to protect humans from coercion, deceit, manipulation, conditioning, or herding, thereby ensuring that self-rule, self-governance, or self-determination is not compromised by AI systems.¹³ The threats posed by AI systems to human autonomy can manifest in various ways, such as direct interference with human agency by limiting a person's negative freedom. It is important to note that relevant negative freedoms vary significantly depending on the technology and use context. For instance, technologies that exert considerable influence on the physical environment can interfere with individuals' physical functions and mobility.¹⁴ However, when these technologies are used in virtual environments to impact physical functions, this risk is amplified. For example, in a workplace setting, AI-driven monitoring systems can restrict employees' actions by constantly surveilling and analysing their productivity.¹⁵ Similarly, in educational environments, AI-powered learning platforms might constrain students' learning paths by automatically determining what they should study next, limiting their ability to explore

¹¹ HLEG guidelines, Executive Summary, p.2.

¹² *ibid.*

¹³ Arto Laitinen and Otto Sahlgren, 'AI Systems and Respect for Human Autonomy' (2021) 4 *Frontiers in Artificial Intelligence* <<https://www.frontiersin.org/articles/10.3389/frai.2021.705164>> accessed 8 June 2024.

¹⁴ van der Krabben, E., Kooij, H.-J., Raaphorst, K., & Hoekman, R. (2023). The Impact of the Built Environment and Social Environment on Physical Activity: A Scoping Review. *International Journal of Environmental Research and Public Health*; R. Acheampong, T. C. Balan, D.-M. Popovici, and A. Rekeraho, "Embracing XR System Without Compromising on Security and Privacy," in *Extended Reality*, L. T. De Paolis, P. Arpaia, and M. Sacco, Eds., in *Lecture Notes in Computer Science*. Cham: Springer Nature Switzerland, 2023, pp. 104–120. doi: 10.1007/978-3-031-43401-3_7

¹⁵ Aloisi A and Gramano E, 'Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context Automation, Artificial Intelligence, & Labor Law' (2019) 41 *Comparative Labor Law & Policy Journal* 95



topics independently.¹⁶ This risk is even greater in XR, where AI can influence the virtual space and impact users' physical interactions and movements in high risk environments.

In addition, AI systems can be used to coerce, manipulate, and deceive by removing meaningful options from users or offering options that are difficult to refuse, such as through recommender systems.¹⁷ However, it is important to note that AI systems do not inherently undermine autonomy. Specific factors, such as lack of transparency and hyper-nudging, can contribute to the incursion of AI on human autonomy. Therefore, addressing autonomy issues is crucial to ensure that AI systems support rather than compromise human autonomy.¹⁸

Another significant risk indicating how AI systems can undermine human autonomy is through nudging and paternalism. It should be noted that nudging, even if intended to advance the interests of the recipient, is morally contentious. This "benevolent paternalism" must be justified by meeting four conditions:¹⁹

1. **The Harm Condition:** Interference is justified in the face of substantial and preventable harm or loss.
2. **The Likelihood Condition:** Such interference is highly likely to prevent the harm or loss.
3. **The Weight Condition:** The likely benefits due to interference outweigh the interference-related risks or harms.
4. **The Minimal Interference Condition:** The chosen form of interference is the least restrictive one necessary for securing the expected benefit or mitigating harm.

This concept of benevolent paternalism can be directly connected to the ethical principle of harm prevention highlighted in the guidelines for trustworthy AI.²⁰ While these four conditions may not all be directly relevant to the use cases of the avatar generation component of CORTEX², they are particularly pertinent for avatar generation as a foundational technology as

¹⁶ Barrios Tao H, Pérez V and Guerra Post Ph.D. Y, '2019 72(12) 30 ARTIFICIAL INTELLIGENCE AND EDUCATION Challenges and Disadvantages for the Teacher 1' (2019) 72 Arctic medical research 30

¹⁷ HLEG guidelines, p.12

¹⁸ Laitinen and Sahlgren, p.10.

¹⁹ *ibid*, p.9.

²⁰ *Ibid*, p.9.



well as for NLP and the integration of recommender systems in the use cases developed or deployed in CORTEX². Ensuring these four conditions are met can help mitigate the risks associated with AI systems, thereby protecting human autonomy.

There are other potential risks to human autonomy, such as cognitive heteronomy and direct misrecognition. However, the purpose of this deliverable is to focus on the role of ethics in addressing these issues rather than discussing all possible risks in detail.

2.1.3. The principle of harm prevention

Pursuant to the HLEG guidelines, the principle of harm prevention seeks to ensure the protection of human dignity, physical, and mental integrity. This is particularly relevant when systems can amplify power imbalances or information asymmetry, such as in an employer-employee relationship.²¹ CORTEX2 is to be deployed in work environments where these imbalances are prominent. Therefore, it is crucial to ensure that the AI components are technically robust to prevent misuse, and the needs of those vulnerable to such systems must be taken into account in their development, deployment, and use.

2.1.4. Principle of fairness:

The HLEG guidelines state that fairness involves ensuring that individuals and groups are free from unfair biases and discrimination.²² It requires AI practitioners to respect the principle of proportionality, balancing the means with the desired ends while carefully considering competing interests and objectives. Fairness also entails allowing individuals to contest and seek effective redress against decisions made by AI systems and the humans who operate them. In the context of CORTEX2, it is essential that employees have the ability to contest the decisions of AI systems and the people who operate them.

2.1.5. Principle of explicability

Regarding the principle of explicability, the core requirement is transparency. The capabilities and purposes of AI systems, as well as their decisions, must be explainable so that such decisions can be contested when necessary. When explanations are impracticable due to the

²¹ HLEG guidelines, p.12.

²² *ibid* p.12.



opacity of black-box algorithms, other explicability measures such as traceability, auditability, and transparent communication of system capabilities should suffice.²³

Therefore, CORTEX² must ensure that the functionalities and capabilities of the AI components are fully disclosed, it is important to not that the functionalities and capability are of the various AI components are disclosed in deliverable D5.1. In cases where third-party AI systems are integrated into the framework, it is crucial to ensure that these parties also disclose the capabilities and purposes of their AI systems. Third parties have made disclosures in their proposal, while selected candidates will be required to provide a more details documentation of any AI component to be co-developed. It is recommended that disclosures about the use of deepfakes and conversational agents, as well as training and awareness programs, should be integrated into deployment and adoption efforts to support explainability. Additionally, establishing monitoring and accountability mechanisms would be beneficial to achieve the other explicability measures identified in this section.

2.2. Requirements for Trustworthy AI

To achieve these principles, the High-Level Expert Group (HLEG) has compiled a non-exhaustive list of requirements, along with technical and non-technical measures, to facilitate their implementation throughout the lifecycle of AI systems. For these requirements to be effectively met, developers, deployers, end-users, and society each have various roles to play. Developers are responsible for integrating these requirements during the design and development phases. Deployers must ensure that the AI systems they use or offer to others comply with these requirements. End-users and the general public should be informed about these requirements and should actively demand their implementation.

This cohesion among developers, deployers, end-users, and society is essential for achieving a more responsible and ethical implementation and use of AI systems.²⁴ Such collaboration can enhance the safety, fairness, and societal acceptance of AI technologies. The seven requirements are discussed below.²⁵

²³ Hleg guidelines; Madrid AP y and Wright C, Trustworthy AI Alone Is Not Enough (ESIC 2023).

²⁴ HLEG guidelines, p.13.

²⁵ *ibid*, p14.

- 1. Human Agency and Oversight:** AI systems are required to support users' autonomy and decision-making while safeguarding fundamental rights and allowing for human oversight. It is recommended that a Fundamental Rights Impact Assessment (FRIA) be conducted in high-risk scenarios involving AI systems. The FRIA evaluates the possibility of mitigating the risks associated with the AI system or determining whether the risks are justifiable in a democratic society in order to respect the rights and freedoms of others.²⁶ Conducting an FRIA is also required by the AI Act and highly recommended in this deliverable. Additionally, users must be well-informed to make well-guided choices about their interactions with AI systems. Human oversight should also be established as a governance mechanism for AI systems, in one of the following configurations: human-in-the-loop, human-on-the-loop, or human-in-command.²⁷ Each configuration requires varying levels of human intervention in the decision-making cycle of AI systems, ensuring that ethical and responsible use is maintained.²⁸
- 2. Technical robustness and safety:** this requirement aligns with the ethical principle of harm prevention, which involves taking a preventive or precautionary approach to risks to minimize unintended and unexpected harms while preventing unacceptable ones.²⁹ Consequently, AI systems must be resilient to attacks and secure enough to restrict dual-use and potential abuse. Additionally, AI systems should have fallback plans and general safety protocols in place for when issues arise, with the required level of safety depending on the severity of the risks posed by the AI system.³⁰ AI systems must operate with a high level of accuracy, especially when human lives are at stake. When inaccuracies are unavoidable, the likelihood of such inaccuracies must be disclosed. Technical robustness also entails that the results of AI systems be reliable and reproducible.

²⁶ HLEG guidelines, p15.

²⁷ *ibid*, p. 16

²⁸ *ibid*.

²⁹ *ibid*.

³⁰ *Ibid*,



3. **Privacy and data Governance:** this requirement is closely connected to the principle of harm prevention.³¹ This requirement revolves around ensuring adequate data governance regarding the quality and integrity and data used in AI systems. Therefore AI Systems must prioritise privacy and data protection, as well as the use of quality training data to safe guard against biases and factual inaccuracies. The various data sets used and the processes used on such data must be tested and document.³² Accessing quality training datasets for AI models is a current challenge due to the ethical issues it raises. For instance, AI models are now often trained with publicly available videos on platforms like YouTube.³³ While this practice violates the terms of service, it remains a grey area that requires more attention, given that individuals appearing in such videos could not have anticipated their data being used for AI training. Transparency, fairness, and accountability are ethical imperatives that could assist in addressing this challenge. It should be noted that general-purpose AI must meet the documentation and transparency obligations imposed by AI regulations, which can help prevent the misuse of training data sourced from publicly available personal data. These documentation and transparency requirements are discussed elsewhere in this deliverable.
4. Transparency is linked to the ethical principle of explicability and concerns relevant details such as data, system functionality, and business models.³⁴ Transparency can be achieved through the implementation of traceability measures, which include documenting datasets, their collection methods, annotation processes, and usage. Additionally, the decision flow of AI systems must be documented to ensure transparency. This documentation facilitates the identification of the roots of erroneous AI decisions and serves as a guardrail for preventing future mistakes.

Another critical aspect of implementing transparency is ensuring that both technical processes and related human decisions can be understood by human beings. When AI

³¹ bid, p.17.

³² HLEG guidelines, p.17.

³³ Kerem Gülen, 'OpenAI Used YouTube Videos To Train AI, Report Claims - Dataconomy' (8 April 2024) <<https://dataconomy.com/2024/04/08/openai-used-youtube-videos-to-train-ai-report-claims/>> accessed 21 June 2024.

³⁴ HLEG guidelines, p.18.



systems have significant impacts on human lives, explanations should be timely and tailored to the expertise of the concerned stakeholders (e.g., laypersons, regulators, or researchers).³⁵ Moreover, AI systems must be identifiable by the humans they interact with, and the capabilities and limitations of the AI systems should be communicated to AI practitioners or end-users in a manner appropriate to the specific use cases³⁶. With regard to the generative AI in CORTEX² capable of generating deepfakes and for conversational agents, it must be clearly disclosed that the virtual assistant is an AI.

5. **Diversity, non-discrimination and fairness:** this requirement is closely linked to the ethical principle of fairness. Fairness entails that all affected and relevant stakeholders are included throughout the process, ensuring equal access and treatment.³⁷ A crucial aspect of this requirement is the elimination of unfair bias. To prevent such bias, identifiable and discriminatory biases should be removed at the data-gathering stage. Promoting diversity in recruitment and implementing oversight processes to analyse and address the purpose, constraints, requirements, and decisions of the AI system transparently can help counteract algorithmic bias.

Moreover, these technologies must be accessible to individuals with disabilities.³⁸ Stakeholder participation is essential for creating a fair and inclusive AI system, and this can be achieved through regular feedback from stakeholders throughout the AI systems' lifecycle. Notably, some of these accessibility requirements were incorporated during the design phase. For instance, the CORTEX² Conversational Agent not only responds to voice prompts but also recognizes written prompts and gestures, allowing for customization of prompts as discussed during the co-development triage.

6. **Societal and environmental well-being:** another requirement connected to the principles of fairness and harm prevention is to consider societal and environmental

³⁵ *ibid.*

³⁶ HLEG guidelines, p.18.

³⁷ *ibid.*

³⁸ *ibid.*, pp. 18-19.

well-being throughout the lifecycle of the AI system.³⁹ Achieving sustainability should be at the forefront of the development, deployment, and use processes. This includes a critical evaluation of resource usage and energy consumption during training.⁴⁰ Additionally, it is essential to assess the social impact dimension, including the effects on society and democracy.

It is pertinent to mention that the reduction of energy consumption was one of the promises of the CORTEX² project, which is closely linked to the societal and environmental well-being requirement. However, specific steps must be taken to determine or support the actual determination of the energy savings arising from the use of AI for facial re-enactment. This assessment will help ensure that sustainability goals in the CORTEX² project are met and contribute positively to societal and environmental well-being.

7. **Accountability:** Lastly, but certainly not least, is the accountability requirement, which is closely connected to the principle of fairness and supports the other requirements for trustworthy AI.⁴¹ Accountability ensures that responsibility for the outcomes, both pre- and post-development, deployment, and use, can be appropriately allocated. To achieve accountability, auditability is essential; this means that algorithms, design processes, and data must be assessable.⁴² For accountability to be effective, it should be possible to report and respond to negative outcomes, identify, assess, document, and minimize impacts—especially for affected individuals—protect whistle-blowers, and use appropriate impact assessments.⁴³ When these requirements for trustworthy AI conflict, leading to inevitable compromises, such compromises must be reached in a rational and methodological manner. With regard to CORTEX2 the algorithms must be auditable throughout the lifecycle, design, development and deployment

³⁹ *ibid*, p.19.

⁴⁰ *ibid*.

⁴¹ HLEG guidelines, p.19-20.

⁴² *ibid*.

⁴³ *ibid*, p.20.



2.3. Ethics in XR

Ethics in XR is emerging. However, based on the preliminary ethical requirements identified in Section 2 of deliverable D4.1 and the analysis of relevant literature on fundamental rights and fairness perspectives, the following have been identified as the most relevant and recurring ethical themes in XR technology: autonomy, dignity, transparency, equality, diversity and inclusion. Without much repetition, some of the issues arising from these ethical themes and their relevance to CORTEX² are discussed below:⁴⁴

- 1. Healthy and Safety:** concerns like cyber sickness are one of the main issues with XR technologies. Cyber sickness can severely undermine the user experience and can manifest in various ways and severities.⁴⁵ In the event of cyber sickness or other health and safety hazards, it is essential to determine beforehand how CORTEX² participants will receive assistance during the experiments.
- 2. Challenges to agency and autonomy:** numerous autonomy issues have been identified in this deliverable. The functioning of various XR technologies and their applications significantly impacts user agency and autonomy.⁴⁶ Workplace AR systems, for instance, could exploit workers' data, influencing their agency and assessing their emotional states without their knowledge, raising serious concerns about workplace autonomy.⁴⁷ Additionally, XR advertisements often use manipulative techniques like emotional persuasion, deception, and false advertising, exploiting consumer vulnerabilities. When using XR for remote work, it is crucial to ensure that techniques undermining user autonomy are not integrated into CORTEX² by the consortium or any third parties.
- 3. Accessibility and Inclusivity:** XR technologies face significant accessibility and inclusivity challenges, as highlighted in various studies.⁴⁸ These challenges

⁴⁴ Meenaakshisundaram K, 'The Ethics of Extended Realities: Insights from a Systematic Literature Review' 2023; Vallor S, Raicu I and Green B, 'Technology and Engineering Practice: Ethical Lenses to Look Through' [2020] Markkula Center website

⁴⁵ Vallor, Raicu and Green, 'Technology and Engineering Practice: Ethical Lenses to Look Through' [2020] Markkula Center website p18

⁴⁶ Vallor, Raicu and Green, p.21.

⁴⁷ Greene J, 'Ethical Design Approaches for Workplace Augmented Reality' (2023) 10 Commun. Des. Q. Rev 16.

⁴⁸ Vallor, Raicu and Green pp.26-27.



encompass both physical and non-physical elements. For example, head-mounted displays (HMDs) used in XR can cause discomfort for individuals who wear glasses, impacting those with visual impairments such as myopia, hyperopia, or color blindness.⁴⁹ Additionally, persons with Autism Spectrum Disorder (ASD) find it difficult to use HMD controllers, especially those with psychomotor or cognitive impairments, raising concerns about the effectiveness of VR interventions for this group. Addressing these issues is crucial to ensure that XR technologies are accessible and inclusive for all users.⁵⁰ CORTEX² has been evaluated for other relevant accessibility and inclusivity constraints to identify potential vulnerable groups and accessibility requirements. As a result, the CORTEX² framework has incorporated design requirements to enable various user groups, regardless of disability, to interact with the conversational agent in CORTEX². In addition, all results displayed in CORTEX² are being adapted to ensure they meet various visual and cognitive standards for persons with disabilities. More accessibility and inclusivity issues may be discovered during the testing phase, which can then be addressed to improve the adoption phase. Stakeholder engagement has proven useful in integrating accessibility and inclusivity requirements into the solutions proposed in Open Call 1.

Recommendations

1. Perform Fundamental Rights Impact Assessments (FRIAs) for high-risk AI applications to identify and mitigate potential ethical issues.
2. Regularly review AI systems for biases and take corrective actions to ensure fairness and non-discrimination.
3. Enhance transparency and explainability by documenting and communicating the capabilities and limitations of AI systems,

⁴⁹ *ibid.*

⁵⁰ *ibid*



	<p>including those developed by third parties, to users clearly and effectively.</p> <ol style="list-style-type: none"> 4. Partners involved in developing AI components in WP3 must disclose details of the provenance of their train, testing and validation data sets. 5. Develop and implement protocols to manage risks like cybersickness and other health hazards in XR environments, especially during testing phase. 6. Design XR interfaces to be accessible to users with disabilities and continuously update these designs based on stakeholder feedback throughout the lifecycle of CORTEX². 7. Provide feedback on the actual or projected energy savings resulting from the use of AI for facial re-enactment and other functionalities within the CORTEX² project as opposed to image streaming.
--	---

3. Privacy and data protection

In developing XR technologies, particularly for workplace applications, it is crucial to prioritize privacy and data protection. The processing activities in CORTEX² must adhere to the GDPR's data protection principles and respect the rights of data subjects. Ensuring compliance with GDPR not only protects data but also builds trust and confidence among users. By embedding these principles into XR technologies, organizations can create a secure and privacy-preserving environment for all stakeholders. In Section 3 of Deliverable D4.1, a brief introduction to the data protection principles was provided. This deliverable further examines these principles and explores their application to CORTEX².



3.1. Data Protection Principles

Given the wide range of personal and non-personal data categories in CORTEX², which can be combined to derive insights about individuals, it is imperative to strictly adhere to data protection principles. The GDPR outlines the key principles that must be followed to ensure privacy and the protection of personal data. This section will first briefly explain these principles and then discuss their application to the CORTEX2 project in detail.

1. Lawfulness, Fairness, and Transparency: data processing must be legal, fair, and transparent to data subjects.⁵¹
2. Purpose Limitation: data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.⁵²
3. Data Minimization: only data that is necessary for the purposes for which it is processed should be collected and retained.⁵³
4. Accuracy: data must be accurate and kept up to date, with inaccuracies corrected or deleted without delay.⁵⁴
5. Storage Limitation: data should be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed.⁵⁵
6. Integrity and Confidentiality (Security): data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.⁵⁶
7. Accountability: compliance with these principles must be demonstrated, with the ability to provide evidence of such compliance.⁵⁷

⁵¹ Article 5(1)(a) GDPR.

⁵² Article 5(1)(b) GDPR.

⁵³ Article 5(1)(c) GDPR.

⁵⁴ Article 5(1)(d) GDPR.

⁵⁵ Article 5(1)(e) GDPR.

⁵⁶ Article 5(1)(f) GDPR.

⁵⁷ Article 5(1)(2) GDPR.



3.1.1. Lawfulness Fairness and Transparency

Ensuring that XR technology for remote work complies with data protection principles is crucial. This includes adhering to the principle of lawfulness, which can be based on consent, contractual necessity, legal obligations, the protection of vital interests, public interest tasks, or legitimate interests that do not override the rights of data subjects. Understanding the potential for privacy breaches in XR highlights the importance of these principles.

CORTEX² envisions use cases across various domains, including education, business, industry, healthcare, emergency and crisis management, entertainment and culture, smart cities, accessibility, and social inclusion. This diverse range of applications highlights both the benefits of XR and the necessity for robust data protection measures. It is important to note that consent is not a suitable legal basis in the context of employment due to the inherent power imbalance. In all other scenarios anticipated in CORTEX², an appropriate legal basis must be determined on a case-by-case basis. By recognizing the potential for privacy breaches and emphasizing the importance of data protection, CORTEX² aims to ensure the responsible and ethical deployment of XR technology.

3.1.2. Purpose Limitation

It is crucial to note that personal data must be processed for specified, explicit, and legitimate purposes, as mandated by the principle of purpose limitation under the GDPR.⁵⁸ When further processing of personal data is considered, such additional processing must be compatible with the initially specified, explicit, and legitimate purpose. For example, if personal data is initially processed for educational or worker training purposes, using the data for advertising, workplace surveillance, contesting workplace accident claims, or other incompatible purposes would be unlawful under the GDPR.

The Cortex2 project exemplifies compliance with the principle of purpose limitation by outlining several explicit purposes for data collection and processing. These purposes include:

1. Providing XR experiences as an extension of videoconferencing systems.

⁵⁸ Key sections of the GDPR include Article 5(1)(b), which establishes the principle of purpose limitation, and Recital 50.

2. Developing resource-efficient teleconferencing tools.
3. Integrating Internet of Things (IoT) devices for optimised interaction.

These detailed and specific purposes ensure that data collection aligns with the project's objectives. Consequently, all co-development endeavours of the core Cortex components must also adhere to this principle of purpose limitation.

Furthermore, the evaluation and selection of third parties for the co-development of the core CORTEX² components and enabling technologies have been conducted with the purpose limitation principle in mind. This ensures that all collaborative efforts to develop the core components of CORTEX² remain compliant with GDPR provisions.

3.1.3. Data minimisation principle

This principle requires that personal data collection be adequate, relevant, and limited to what is necessary for its intended purposes.⁵⁹ It ensures that data processing does not excessively interfere with the interests, rights, and freedoms of individuals. Personal data should only be processed when essential to achieve a legitimate purpose and should not be undertaken if the purpose can be reasonably achieved by other means. This ensures that data processing is proportional and protects individuals' rights and freedoms. The European Court of Justice (ECJ) underscored the importance of data minimisation in the Digital Rights Ireland case,⁶⁰ which examined the Data Retention Directive. The Directive was deemed problematic because it adopted a broad approach to data retention, encompassing all individuals and all types of electronic communication without differentiation, in the context of combating serious crime.

CORTEX² collects various types of personal data, including voice, image, motion, and gesture data, to create realistic and interactive avatars, support multimodal conversational interactions, and provide comprehensive meeting summarisations. The CORTEX² project has carefully evaluated the types of data collected to ensure that only the minimal amount necessary for the intended purpose is processed. For example, when collecting facial images for avatar generation, only the data necessary to create an accurate user avatar is processed. Collecting

⁵⁹ Articles 5(1)(c) and 25(2) GDPR.

⁶⁰ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECJ Joined Cases C293/12 and C594/12.



additional data, such as retina scans and eye-tracking information, would be unnecessary and contrary to the principle of data minimization. In addition, in using the YouTube videos to train the AI models, facial images are cropped to ensure that only hand movements are being analysed.

In meeting summarization, CORTEX² transcribes conversations in real-time and generates concise summaries, avoiding the need to store entire transcripts or video recordings. This approach enhances the efficiency of data processing and limits the collection of unnecessary personal data. Through these measures, CORTEX² demonstrates the data minimisation principle by ensuring that the data collected is adequate and relevant to its specified purposes.

3.1.4. Accuracy Principle

The GDPR accuracy principle, stipulated in Article 5(1)(d), mandates that personal data must be accurate and, where necessary, kept up to date. This principle is crucial for projects handling personal data, as inaccuracies can lead to significant consequences for individuals, including wrongful decisions based on erroneous information, such as errors in meeting summarization.

The accuracy principle is particularly relevant for the generation of avatars and the reconstruction of 3D objects in XR environments like CORTEX². There is an ongoing debate about ensuring avatars accurately represent the physical attributes of data subjects while allowing users to alter their appearances in the virtual world to match their identity.⁶¹ Users of XR technology face identity-related concerns due to AR applications enabling significant modifications to their appearance, leading to privacy risks, social repercussions, and potential loss of employment.⁶² Additionally, ethical dilemmas arise in virtual environments, where avatars often lack realism and emotional expression, thus affecting social interactions and the overall user experience.⁶³

⁶¹ D. Hosfelt, "Making ethical decisions for the immersive web." arXiv, May 14, 2019. doi: 10.48550/arXiv.1905.06995.

⁶² De Felice F and others, 'Physical and Digital Worlds: Implications and Opportunities of the Metaverse' (2023) 217 *Procedia Comput. Sci.* 1744.

⁶³ Baker S and others, 'Interrogating Social Virtual Reality as a Communication Medium for Older Adults' (2019) 3 *Proc. ACM Hum.-Comput. Interact.* 149:1.



Moreover, the accuracy principle applies to AI-enabled components of XR, underscoring the need for AI to function as precisely as possible.⁶⁴ The importance of AI accuracy is heightened in high-stakes scenarios such as factories, healthcare, and emergency management, where inaccuracies can cause significant harm. Therefore, the obligation to ensure data accuracy must be understood in the context of the data processing purpose.⁶⁵ The required level of data accuracy is directly connected to the intended purposes of such processing, especially where inaccuracies in AI models can lead to physical or mental harm and unfair outcomes.

The integration of AI and machine learning technologies in the project, such as gesture recognition, must be carefully managed to avoid inaccuracies. Additionally, accuracy is relevant for interactions with conversational agents, ensuring that the AI provides accurate results.

3.1.5. Storage Limitation Principle

The Storage Limitation Principle provides that personal data should only be stored for as long as necessary. This is particularly crucial when data is retained in a form that permits the identification of data subjects. Data retention can be extended for archival purposes in the public interest, or for scientific, statistical, or historical research, provided that suitable technical and organizational measures are implemented in line with Article 89(1) GDPR. Once personal data has served its purpose, it should be securely deleted or anonymised to guarantee the right to privacy of data subjects. These requirements are especially pertinent for the personal data used in immersive technologies and enabling technologies in XR.

The CORTEX² project has established clear retention policies and integrates mechanisms for the timely review and deletion of data. This approach aligns with the GDPR, effectively managing the data lifecycle and reducing the risks of data breaches and misuse. From the data management plan, it is evident that the project places a strong emphasis on retaining personal data only for as long as necessary.

To further protect user privacy, the CORTEX² project plans to employ data anonymisation techniques. These methods are particularly important for data that must be retained for

⁶⁴ K. Smit, M. Zoet, and J. V. Meerten, "A Review of AI Principles in Practice," presented at the Pacific Asia Conference on Information Systems, 2020.

⁶⁵ C. Giakoumopoulos, G. Buttarelli, and M. O'Flaherty, pp. 127-128; CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 May 2009.

extended periods for research and development purposes. The specific anonymisation techniques to be used should be determined in advance to ensure compliance and effectiveness. Currently, third parties have been invited to develop privacy-preserving solutions for the CORTEX² project, highlighting the need to specify the most suitable techniques beforehand.

By reinforcing data retention policies, employing advanced computing architectures, anonymising personal data, managing the data lifecycle effectively, and adhering to strict legal and ethical standards, the CORTEX² project demonstrates a strong commitment to safeguarding personal data and adhering to existing and impending regulatory requirements.

3.1.6. Integrity and Confidentiality

Concerning implementing the appropriate technical and organisational measures, the integrity and confidentiality principles require that data controllers ensure protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.⁶⁶ In the context of XR, it is pertinent to implement measures to prevent impersonation and unauthorized access to personal data harvested from XR technologies. For instance, through the use of encryption, access control and multi-factor authentication. However, even with the aforementioned principles in place, data processors and controllers, in line with the accountability principle must be able to demonstrate compliance with these principles to data subjects and supervisory authorities.⁶⁷ The CORTEX² project demonstrates due consideration for integrity and confidentiality principle through its secure-by-design architecture, robust data encryption techniques, and strict access control measures such as Keycloak for IoT authentication. However, for future use of this technology regular audits and reviews, and a comprehensive incident response plan would be beneficial.

3.2. Data Subject Rights

The incorporation of XR technologies into remote work holds significant promise for the future workplace but also demands meticulous attention to the data subject rights outlined in the

⁶⁶ Art. 5(1)(f), GDPR.

⁶⁷ Art. 5(2), GDPR.



GDPR. These rights encompass (1) the right to be informed, (2) the right of access, (3) the right to rectification, (4) the right to erasure, (5) the right to restrict processing, (6) the right to object, (7) the right to withdraw consent, (8) the right to data portability, (9) the right to object to automated decision-making, and (10) the right to lodge complaints.⁶⁸ To exercise these rights, the data subject must submit a request to the controller or processor, who is then legally obligated to address the request. It is important to note that some of these rights do not require a formal request from data subjects; instead, the controller must proactively implement measures, such as the right to be informed, regardless of whether the data subject chooses to exercise their right.⁶⁹ These rights are discussed below in relation to the CORTEX² project.

3.2.1. Right to be Informed

This right is linked to the transparency branch of the three-pronged principles of lawfulness, fairness, and transparency. Article 12(1) GDPR seeks to ensure the controller takes appropriate measures to provide data subjects with all information and communications regarding the processing of personal data, as specified in Articles 13 and 14, Articles 15 through 22 and 34 of the GDPR, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Under this right, data subjects are to be notified of the identity of the controller and processor, the legal basis and purpose of such processing, the various categories of data being processed, how they are processed, and the consequences, safeguards and rights regarding such processing, the recipients of the data, the storage period of the data or the criteria for determining the duration of storage, the existence of automated decision-making, including profiling, and the source of any personal data not obtained directly from the data subject.⁷⁰ This right can be relevant in employment relationships, especially in the context of XR solutions for remote work where various data is collected and transmitted across countless platforms or applications. It is essential to inform the employees of the relevant information and communications stipulated in the GDPR.

⁶⁸ C. Giakoumopoulos, Buttarelli, and O’Flaherty, pp. 206-207

⁶⁹ S. Schöbel, A. Schmitt, D. Benner, M. Saqr, A. Janson, and J. M. Leimeister, “Charting the Evolution and Future of Conversational Agents: A Research Agenda Along Five Waves and New Frontiers,” *Inf Syst Front*, Apr. 2023, doi: 10.1007/s10796-023-10375-9.

⁷⁰ Art. 12, GDPR; Art. 15, GDPR.



The integration of XR technologies, such as Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR), into remote work environments presents significant advancements in collaboration, training, and productivity. However, this integration necessitates careful attention to the transparency obligations stipulated under the GDPR's right to be informed.

This right is a key element of the GDPR's principles of lawfulness, fairness, and transparency. Article 12(1) of the GDPR mandates that data controllers take appropriate measures to provide data subjects with all necessary information regarding the processing of their personal data. This information must be conveyed concisely, transparently, intelligibly, and in an easily accessible form, using clear and plain language, as specified in Articles 13, 14, and 15-22, as well as Article 34 of the GDPR. Under this right, data subjects must be informed about the identity of the controller and processor, the legal basis and purpose of processing, the categories of data being processed, the processing methods, the consequences, safeguards, and rights associated with the processing, the recipients of the data, the storage period or criteria for determining this duration, the existence of automated decision-making, including profiling, and the source of any personal data not directly obtained from the data subject. This right is crucial in employment contexts, particularly with XR solutions for remote work, where various types of data are collected and transmitted across multiple platforms or applications. It is essential to inform employees of the relevant information and communications as stipulated in the GDPR.

In the context of XR technologies, these requirements are particularly pertinent. XR applications often involve the collection and processing of substantial amounts of personal data, including biometric data, location data, and behavioural data. For example, VR headsets may track eye movements, facial expressions, and physical gestures to enhance the immersive experience, while AR applications might collect data from the user's environment to overlay digital information accurately.

To comply with the right to be informed stipulated in the GDPR, organisations adopting XR technologies in remote work must ensure that employees are fully aware of the data being collected and how it is used. This includes:



1. Identity of the Controller and Processor: Clearly informing employees about who is responsible for data collection and processing in XR applications.
2. Legal Basis and Purpose of Processing: Explaining why the data is being collected and processed, such as for improving user experience or providing on-the-job training.
3. Categories of Data: Specifying the types of data collected, which may include biometric data, behavioural data, interaction data, and environmental data.
4. Processing Methods: Detailing how the data is processed, stored, and protected, including any automated decision-making processes involved.
5. Rights and Safeguards: Informing data subjects about their rights under the GDPR, including the right to access, correct, and delete their data, and the measures in place to protect such data.
6. Data Recipients: Identifying any third parties with whom the data may be shared, such as cloud service providers or analytics partners.
7. Storage Period: Indicating how long the data will be stored or the criteria used to determine this duration.
8. Automated Decision-Making: Disclosing any use of automated decision-making, including profiling, within the XR applications.
9. Data Sources: For any data not collected directly from the data subject, explaining the source of this data is necessary.

3.2.2. Right of Access⁷¹

Under this right, data subjects are entitled to request information about the processing of their personal data. This includes details about the purpose of the processing, the categories of data involved, the recipients of the data, storage periods, and the right to request rectification or erasure of personal data. Additionally, they have the right to restrict or object to the processing

⁷¹ Art. 13 -14, GDPR.



of their data. Under this provision of the GDPR, data subjects can also request confirmation of their right to lodge a complaint and inquire about the existence of automated decision-making.

The controller is obligated to provide the data subject with the actual identity of the recipients of their personal data unless it is impossible to identify those recipients. However, if the requests made by data subjects for access are proven to be manifestly unfounded or excessive, as defined in Article 12(5) GDPR, the controller may refuse to provide this information.⁷²

Regarding the experimental phase of CORTEX², it is necessary to provide a mechanism for participants to request access to their data. This can be achieved through a dedicated contact point designated at the point of obtaining consent. Additionally, there should be project-wide specifics about how access will be provided to data subjects, such as through digital means, in a commonly used electronic format.

3.2.3. Right to rectification

This right allows data subjects to promptly correct inaccurate or incomplete personal data, aligning with the accuracy principle.⁷³ Notably, data subjects can usually request rectification of minor data errors; however, for legally significant information, proof of inaccuracy may be required, provided this burden is not unreasonable.⁷⁴ In the context of XR, while it might be possible for data subjects to correct inaccuracies in their avatars, identifying and rectifying specific inaccuracies in behavioural data can be more challenging. This difficulty arises because for instance, avatar generation relies on intrinsic data, such as facial images,⁷⁵ whereas behavioural data, like eye-tracking and gait analysis, are derived from monitoring data subjects' actions and interactions.

Regarding the exercise of this right in CORTEX², there should be a detailed procedure for data subjects to request rectification of their personal data. This requirement must also extend to the various use cases in the project.

⁷² Article 15, GDPR.

⁷³ Article 16 GDPR.

⁷⁴ C. Giakoumopoulos, Buttarelli, and O'Flaherty, pp 219-221

⁷⁵ Adhanom IB, MacNeilage P and Folmer E, 'Eye Tracking in Virtual Reality: A Broad Review of Applications and Challenges' (2023) 27 Virtual Reality 1481.



3.2.4. Right to Erasure (right to be forgotten)

The right to erasure, as stipulated in Article 17 of the GDPR, can be exercised under specific conditions. These conditions include when erasure is required by Union or Member State law, when the processing of personal data is unlawful, when personal data is no longer necessary for the purposes for which it was collected, or when the legal basis for processing has ceased to exist, such as when consent is withdrawn or the data subject objects to the processing.

Users should be able to exercise this right to request the deletion of their personal data from company databases, including data from XR and remote working tools, such as their avatars or sensitive data contained in meeting summaries. However, for other types of personal data, such as behavioural data collected during training sessions or business meetings, exceptions to the right to be forgotten may apply. These exceptions occur particularly where such processing is necessary for the establishment, exercise, or defence of legal claims.⁷⁶

One major challenge for the CORTEX² experiments is ensuring that third-party components and services integrated into CORTEX² comply with the right to erasure. Achieving this compliance can be facilitated through comprehensive Data Processing Agreements (DPAs) with all third-party providers, clearly outlining their obligations regarding data erasure.

3.2.5. Right to restrict processing

This right allows for a temporary halt in processing personal data under specific conditions, such as when the accuracy of the data is contested, the processing is considered unlawful, the data is needed to defend a legal claim, or the data subject objects to the processing under Article 21(1) of the GDPR.⁷⁷ Similar to the rights to erasure and rectification, there must be a mechanism for data subjects to exercise this right. Given the use of AI components in CORTEX², this right is crucial to ensure that the controller can store the personal data while addressing the dispute in question.

⁷⁶ Article 17(3)(e) GDPR.

⁷⁷ Article 18, GDPR.



3.2.6. Right to object

This right refers to the right of data subjects to protest or oppose the processing of personal data on grounds related to the data subject's peculiar circumstances, where such processing is based on the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; or in pursuit of the legitimate interests of the controller or of a third party.⁷⁸ The data subject is also entitled to object to processing carried out for direct marketing purposes⁷⁹ or processing for scientific or historical research purposes or statistical purposes unless such processing activity is necessary for the performance of a task carried out for reasons of public interest.⁸⁰

CORTEX² collects and processes various types of personal data, including behavioral data, facial data for avatars, and sensor data from IoT devices. Data subjects involved in CORTEX² have the right to object to the processing of their data on the grounds mentioned above. This includes opposing the use of their data for purposes that may not align with their personal circumstances or interests.

When a data subject objects to the processing, the project must halt the specific processing activity unless it can justify the necessity of the processing based on compelling legitimate grounds.⁸¹ This includes ensuring that any processing for public interest tasks or legitimate interests is critically evaluated against the data subject's rights. CORTEX² must establish a clear and accessible procedure for data subjects to exercise their right to object.

3.2.7. Right to withdraw consent

Under this right, data subjects can easily withdraw their consent to data processing at any time without incurring negative consequences and without negating any lawful processing carried out based on consent before the said withdrawal.⁸² This is particularly relevant in situations where employees or users of XR solutions initially consented to data collection via XR

⁷⁸ Article 21 (1), GDPR.

⁷⁹ Article 21 (2), GDPR.

⁸⁰ Article 21(6). GDPR.

⁸¹ Article 6(1)(f), GDPR.

⁸² Article 7(3), GDPR.



technologies used for teleworking. CORTEX² must ensure that mechanisms are in place for individuals to easily withdraw their consent.

3.2.8. Right to Data Portability

Data subjects have the right, free from unreasonable restrictions, to receive and transmit their personal data in a structured, widely-used, machine-readable format when processing of that data is automated and based on consent. Only personal data processed in accordance with a contract or with consent is subject to this right, which is described in Article 20 of the GDPR.

CORTEX² must adopt standardized data formats to facilitate the seamless transfer of data. This includes ensuring that data related to avatars, virtual workspaces, and user interactions can be exported and imported without compatibility issues. CORTEX² must also clearly define the categories of data that are portable and ensure mechanisms are in place to facilitate their transfer.

3.2.9. Right to object to automated individual decision-making

This right inherently bans decisions based exclusively on automated processing, including profiling, that significantly impact data subjects, and it does not require explicit invocation to be effective.⁸³ For instance, data subjects should be able to exercise this right to contest automated decisions made by their employer, such as automated performance reviews or the automatic assignment of tasks based on perceived competence or aptitude as determined or predicted by Automated Decision-Making (ADM) systems. Third parties in CORTEX² must provide clear information about the use of automated decision-making processes, including profiling, in addition to integrating human oversight in decision-making processes that are primarily automated.

3.2.10. Right to lodge complaints with a supervisory authority⁸⁴

Data subjects have the right to file complaints where they reside, work, or where their rights have been violated. In the context of using XR in the workplace, these complaints may pertain to various issues such as excessive workplace surveillance, unfair automated decision-making,

⁸³ Article 22 GDPR.

⁸⁴ Article. 77, GDPR.



or the improper handling of volunteered, observed, and inferred personal data within XR platforms. Specifically, concerning the experiments conducted in the CORTEX² project, data subjects within the purview of consortium partners or third parties must be informed of this right.

3.3. Additional requirements under the GDPR

Complete GDPR compliance requires more than just incorporating data protection principles and protecting data subjects' rights into the creation and application of XR technologies, particularly in distant work environments. It's also crucial to fulfil ancillary obligations including completing Data Protection Impact Assessments (DPIAs), guaranteeing data protection by default, designating a Data Protection Officer (DPO), and keeping track of processing operations, especially when deploying new technologies that may pose high risks to the fundamental rights and freedoms of individuals.⁸⁵ The GDPR mandates a DPIA in cases involving systematic and extensive evaluation of personal aspects based on automated processing, including profiling, that have legal consequences or other significant effects. DPIAs are also necessary in situations involving large-scale processing of special categories of data or data related to criminal convictions and offences, and in the systematic monitoring of a publicly accessible area on a large scale. The widespread adoption of XR technology in public-facing sectors like health, education, public administration, and emergency and crisis management can necessitate DPIAs. Additionally, requirements such as ensuring data protection by default,⁸⁶ the appointment of a Data Protection Officer to carry out compliance functions,⁸⁷ and the recording of processing activities form a triad of additional GDPR compliance requirements geared towards safeguarding the fundamental rights and freedoms of data subjects.

Regarding CORTEX2 deployment, the relevant controller may need to conduct Data Protection Impact Assessments (DPIAs) for large-scale processing activities involving conversational agents. This includes assessing the risks associated with these agents, particularly how they handle speech recognition, natural language processing, and gestures. CORTEX2 already

⁸⁵ Article 35(1) GDPR.

⁸⁶ Article 25 GDPR.

⁸⁷ Article 37 – 39 GDPR.

incorporates privacy-preserving mechanisms such as encryption and access controls. However, third-party co-developers may need to implement additional privacy-preserving measures, especially in high-risk use cases. Partners and third parties involved in processing activities should also document all data processing activities and the purposes of processing.

3.4. Relevant GDPR Roles

The aforementioned principles have significant implications for the core components of CORTEX² and the various use cases envisaged in the project, which involve processing multiple categories of personal data, including behavioural data. Additionally, CORTEX² presents a complex network of actors with various responsibilities concerning privacy and data protection. The key players in CORTEX² are the controllers, processors, and joint controllers.

Based on the main components analyzed and the proposals reviewed during Track 1 of the open call, the relevant data sets in CORTEX² have been identified. These include facial data collected for avatar generation, behavioural data, environmental data from IoT sensors, health data from collaborations with health institutions, location data, communication data, sensor data from wearable devices, operational data, and research data. Therefore, it is crucial to identify the actors responsible for the processing of these data sets.

According to the GDPR, a controller is the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of processing personal data.⁸⁸ If the purposes and methods of processing are dictated by Union or Member State law, the law may also specify the controller or set criteria for their designation. The processor, on the other hand, is a natural or legal person, public authority, agency, or other body that processes data on behalf of the controller.

In the context of CORTEX², the roles of the various parties pursuant to the GDPR are relevant during the pilot, experimentation, and deployment phases of the CORTEX² framework. For instance, the Mediation Gateway in CORTEX², facilitated using Rainbow, will play a key role. The key processing activities include collecting data from various XR modules, IoT devices, and

⁸⁸ Article 4 (7) GDPR.



sensors, and conveying data streams for AR/VR effects or AI voice processing. This generic framework, called the Mediation Gateway, makes the party responsible for the gateway a processor pursuant to the GDPR. The processor must ensure that data is not transferred outside the EU without appropriate safeguards.⁸⁹ Additionally, the processor must keep records of processing activities carried out on behalf of the controller.⁹⁰ The processor will also need to implement appropriate technical and organizational measures to ensure the right level of data security based on the envisaged risk.⁹¹

Regarding the processing activities in the use case and deployment experiments, informed consent or another lawful basis is required to process personal data. Privacy-preserving mechanisms such as access controls and encryption must be implemented to safeguard communication data, user interaction, and behavioural data collected through the Mediation Gateway, ensuring user privacy is protected.

Recommendations

8. Provide clear, concise information about data processing activities, including who is processing the data, why it is being processed, and how it will be used
9. Regularly review data collection practices to ensure they align with the specified purposes.
10. Periodically audit data collection to remove any unnecessary data.
11. Regularly check and update data to maintain accuracy.
12. Establish and enforce policies for how long data is retained, demand similar policies from third parties where necessary.

⁸⁹ Article 28(3)(a) GDPR.

⁹⁰ Article 30(2) GDPR.

⁹¹ Article 32 GDPR.



	<p>13. Use encryption, access controls, and regular security audits to protect personal data.</p> <p>14. Provide clear instructions on how data subjects can exercise their rights.</p> <p>15. Keep detailed records of data processing activities.</p>
--	---

4. Analysis of the AI ACT

The EU AI Act has officially become law. At the time of task T.4.2, the AI Act was still in the proposal stage with an uncertain trajectory and impact on the development of AI systems. However, on May 21, 2024, the Council endorsed the AI Act, setting in motion the next steps in the legislative timeline. The Act will be published in the EU's Official Journal and will enter into force soon.

The AI Act will become effective 20 days after publication, but the timeline for full applicability is 24 months, with specific provisions having different timelines. For instance, the Codes of Practice will become effective 9 months after the regulation takes effect, and the General Purpose AI rules will become applicable 12 months after the Act takes effect.

The section regarding General Purpose AI is particularly relevant for the AI components of CORTEX². This relevance extends to identifying the relevant entities and their corresponding obligations under the AI Act, as well as the specific requirements applicable to CORTEX².

Therefore, it is pertinent to identify these actors pursuant to Article 3 of the AI Act, before determining how the various relevant parties in the CORTEX² value chain fit into these definitions and the specific obligations imposed on them by the AI Act.

4.1. Relevant Actors Pursuant to AI Act

The actors include Provider, Deployer, Distributor, Importer, Authorized Representative, and Product Manufacturer. For clarity, we briefly discuss these roles below:

1. **Provider:** Refers to any natural or legal person, public authority, agency, or other body that develops an AI system or a general-purpose AI model (or has an AI system or model developed) and places it on the market or puts the system into



service under its own name or trademark, whether for payment or free of charge.⁹²

2. **Deployer:** any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.⁹³
3. **Distributor:** any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.⁹⁴
4. **Importer:** any natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established outside the Union.⁹⁵
5. **Authorised representative:** any natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.⁹⁶

4.2. Salient Observations on AI Act trajectory:

Regardless of the applicability of the AI Act to various actors, it is considered best practice for these actors to implement voluntary codes of conduct for requirements under Title III, Chapter 2, which pertain to risk management, data governance, and human oversight, even for AI systems not classified as high risk.⁹⁷

An open question remains: What constitutes personal, non-professional activity in the use of such GPAI or GPAI AI systems? Although this question has yet to be adjudicated in court, some insights can be derived from the “household exemption” under the GDPR, as seen in Maximilian Schrems v.

⁹² Article 3(3) AI Act.

⁹³ Article 3(4) AI Act.

⁹⁴ Article 3(7) AI Act.

⁹⁵ Article 3(6) AI Act.

⁹⁶ Article 3(5) AI Act.

⁹⁷ Article 69 AI Act.



*Facebook Ireland Limited.*⁹⁸ Under the GDPR, activities like using social media for managing personal finances and personal communication are considered non-professional activities, and personal data processing for non-professional purposes is generally exempt from the regulation.⁹⁹

In the context of AI systems used in CORTEX², such as avatar generation and conversational agents, it is crucial to establish specific criteria for what may be considered “non-professional use.” The starting point could be determining that the processing has no connection to professional or commercial activities, trade, or business, and that the processing has limited scope and impact. Third-party partners developing AI components that may be integrated into CORTEX², including collaborators outside of the Union, must also take these criteria into consideration.

4.3. Legal Certainty for General Purpose AI

There have been many attempts to define General Purpose AI (GPAI), but formal definitions for such systems or models remain scarce.¹⁰⁰ The definition in the initial AI Act proposal was heavily criticised for being overly encompassing, including simple image or speech recognition systems.¹⁰¹ In light of this criticism, recommendations were made to describe the AI systems' capabilities more broadly, focusing on both the planned and unplanned uses of such systems, rather than the provider's intention to perform specific functions.¹⁰²

Pursuant to the AI Act, General Purpose AI (GPAI) models need to be clearly defined to ensure legal certainty¹⁰³ General-purpose AI models should be distinctly identified and set apart from AI systems based on their key functional attributes, such as broad applicability and the ability to perform various tasks competently. Making a GPAI model available through an Application Programming Interface (API) is also considered to be placing it on the market.

In the definitions in the initial draft of the AI Act proposal, GPAI was described as an AI system intended by the provider to perform generally applicable functions, such as image and speech

⁹⁸ Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

⁹⁹ Recital 18 GDPR.

¹⁰⁰ Triguero I and others, ‘General Purpose Artificial Intelligence Systems (GPAIS): Properties, Definition, Taxonomy, Societal Implications and Responsible Governance’ (2024) 103 Information Fusion 102135.

¹⁰¹ *ibid.*

¹⁰² *ibid.*

¹⁰³ Recital 97, AI Act

recognition, audio and video generation, pattern detection, question answering, translation, and others.¹⁰⁴ However, for the sake of legal certainty, a clear distinction between GPAI models and GPAI systems has been introduced in the AI Act.

General-purpose AI model: This term refers to an AI model, including those trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks, regardless of how the model is placed on the market. It can be integrated into various downstream systems or applications, except AI models used for research, development, or prototyping activities before they are placed on the market.¹⁰⁵

General-purpose AI system: This term refers to an AI system based on a general-purpose AI model that has the capability to serve a variety of purposes, both for direct use and for integration into other AI systems.¹⁰⁶

By clearly defining these terms, the AI Act aims to provide legal certainty and ensure that both GPAI models and systems are appropriately regulated and distinguished from each other. For instance, in the CORTEX² project, GPAI models are integrated into a framework of other technologies, making the definition of the GPAI model more relevant and applicable.

4.4. Requirement to Implement AI Literacy

With plans to integrate GPAI into CORTEX², providers and deployers of AI systems must take measures to ensure that their staff and other individuals involved in the operation and use of AI systems on their behalf have a sufficient level of AI literacy. This should be done to the best of their ability, considering the individuals' technical knowledge, experience, education, training, and the context in which the AI systems will be used. They should also take into account the persons or groups on whom the AI systems will be applied.

The objective of the CORTEX² project is to provide a comprehensive XR platform that incorporates several AI components, such as GPAI models. These AI technologies will be utilised

¹⁰⁴ Council of the European Union, 'AIA – CZ – General Approach' (25 November 2022) ST 12149 2022 INIT <https://data.consilium.europa.eu/doc/document/ST-12149-2022-INIT/en/pdf> accessed 21 June 2024.

¹⁰⁵ Article 3(63) AI Act.

¹⁰⁶ Art 3(66) AI Act



in various contexts, including industrial remote maintenance, remote technical instruction, and corporate meetings. It is crucial to prioritise AI literacy among consumers and operators in these environments due to several compelling reasons:

1. **Technical Competence:** Users and operators must possess a comprehensive understanding of the functioning of AI components inside the CORTEX² framework in order to efficiently utilise the system and address any problems that may occur. This includes knowledge of AI-driven features such as gesture recognition, speech recognition, and the use of conversational agents.¹⁰⁷
2. **Human-Centered Design:** AI literacy contributes to the development and deployment of AI systems that are user-friendly and meet the needs of various stakeholders. This is particularly important in collaborative environments where multiple users interact with the AI systems simultaneously.¹⁰⁸

4.5. Transparency Requirements

The AI Act imposes transparency obligations on providers and deployers of AI systems, including those in-bred General-Purpose AI (GPAI) models. These obligations are designed to ensure the responsible development, deployment, and use of AI systems, thereby encouraging user confidence and adherence to regulatory requirements.

The AI Act mandates that providers of GPAI models maintain detailed technical documentation, covering training and testing processes, and the results of evaluations of such models. This documentation must be accessible to the AI Office and national competent authorities upon request.¹⁰⁹ In addition, providers must supply relevant information to providers integrating GPAI models into their AI systems, in order to foster a better understanding of the models'

¹⁰⁷ Windelband L, 'Artificial Intelligence and Assistance Systems for Technical Vocational Education and Training – Opportunities and Risks' in Alexandra Shajek and Ernst Andreas Hartmann (eds), *New Digital Work: Digital Sovereignty at the Workplace* (Springer International Publishing 2023) <https://doi.org/10.1007/978-3-031-26490-0_12> accessed 21 June 2024; Walter Y, 'Embracing the Future of Artificial Intelligence in the Classroom: The Relevance of AI Literacy, Prompt Engineering, and Critical Thinking in Modern Education' (2024) 21 *International Journal of Educational Technology in Higher Education* 15

¹⁰⁸ Walter Y, 'Embracing the Future of Artificial Intelligence in the Classroom: The Relevance of AI Literacy, Prompt Engineering, and Critical Thinking in Modern Education' (2024) 21 *International Journal of Educational Technology in Higher Education* 15

¹⁰⁹ Article 53(1)(a) and Annex XI AI Act



capabilities and limitations (Article 53(1)(b), Annex XII). This is relevant for third parties integrating the CORTEX² GPAI.

When GPAI produces synthetic content (text, image, video, or audio) or deepfake, providers are required by Article 50(2) AI Act to make sure that the content has a disclaimer indicating that it was created or altered artificially. The purpose of this rule is to protect end users from deceit and to guarantee openness. Given the unique characteristics and constraints of different contents, the technical solutions for marking AI-generated content must be effective, interoperable, robust, and reliable, considering the specificities and limitations of various content types.¹¹⁰

Recommendations

16. Ensure third-party AI systems integrated into CORTEX² disclose their capabilities and purposes clearly.
17. Regularly review AI systems for biases and discrimination.
18. Provide comprehensive AI literacy training for users involved in operating and interacting with AI systems within CORTEX².
19. Ensure AI systems have fallback plans and safety protocols in place to address potential issues.
20. Maintain detailed records of AI system development, deployment, and monitoring processes.
21. Conduct regular internal audits to ensure ongoing adherence to AI Act requirements and other relevant regulations.
22. Ensure that all AI-generated content, including deepfakes, is clearly labeled. According to the AI Act, providers of AI systems must ensure that synthetic content is accompanied by a disclaimer

¹¹⁰ Recital 134, AI Act



5. Cybersecurity framework for CORTEX²

The advancement in XR technologies has undoubtedly revolutionized telepresence and collaborative workspaces, with the impact of this innovation likely to extend into the physical world. XR systems, which encompass devices that collect and process various data types, are vulnerable to cyber-attacks that can jeopardize user safety and compromise data integrity.

As highlighted in Deliverable D4.1, XR technologies present a multitude of cybersecurity issues stemming from connected devices or IoT, as well as identity and authentication problems, social issues, and physical threats.¹¹¹ Notably, the GDPR and the AI Act contain provisions pertinent to addressing cybersecurity concerns in XR environments.

For instance, Recital 49 of the GDPR emphasizes the importance of maintaining the security and resilience of networks and information systems. Furthermore, Article 32 of the GDPR mandates that data controllers and processors implement appropriate technical and organizational measures to ensure data security. Additionally, the GDPR imposes a notification obligation on controllers regarding personal data breaches.¹¹² According to this article, communication of a personal data breach requires prompt notification to individuals if the breach is likely to result in a high risk to their rights and freedoms.

Considering that the CORTEX² framework also includes GPAIs, it is relevant to review some provisions of the AI Act. The AI Act, specifically tailored to regulate AI, addresses cybersecurity concerns arising from the development and deployment of high-risk AI systems. The AIA emphasizes the need for ensuring that AI systems are resilient to cyber threats and include mechanisms to detect and respond to cyber incidents.¹¹³ The April 2024 final draft of the AI Act stipulates that high-risk AI systems shall be designed and developed to achieve an appropriate level of accuracy, robustness, and cybersecurity. It also mandates that high-risk AI systems incorporate secure development practices, including protection against manipulation and cyberattacks.

¹¹¹ Chow Y-W and others, 'Visualization and Cybersecurity in the Metaverse: A Survey' (2023) 9 Journal of Imaging 11

¹¹² Article 34 GDPR.

¹¹³ Recital 40 AI Act.



5.1. Cybersecurity Concerns Specific to XR Technologies

Studies have shown that XR systems often communicate over the same protocols as the internet, making them susceptible to similar attacks, such as deep fakes and fake identities, which broaden the scope of identity theft.¹¹⁴ Moreover, XR devices, embedded with sensors that track user behaviour, movements, and gaze, pose significant privacy threats.¹¹⁵ For instance, biometric data used in positional tracking can be exploited by third parties, compromising user anonymity and potentially leading to blackmail if anonymous virtual activities are linked to real-world identities. The legislative measures implemented by the EU, including the GDPR and AI Act, play a crucial role in mitigating the cybersecurity risks associated with XR technologies. While the GDPR and AI Act are vital in addressing these risks, the trajectory of XR, especially its use in critical sectors, necessitates considering other more robust cybersecurity regulatory frameworks such as the Cybersecurity Act,¹¹⁶ the NIS2 Directive,¹¹⁷ and the Cyber Resilience Act.¹¹⁸

5.2. Cyber Security Act

The Cybersecurity Act is a landmark piece of legislation in the European Union, designed to significantly bolster the security of information and communications technology (ICT) products, services, and processes across the EU. Enacted in 2019, this Act addresses the escalating cybersecurity challenges brought about by digital transformation and the growing interconnectedness of systems and devices. XR technologies, such as CORTEX2, incorporate various IoT devices and digital ecosystems, including cloud storage and digital infrastructure. Consequently, the Cybersecurity Act is highly relevant to the development and deployment of CORTEX².

¹¹⁴ Acheampong R and others, 'Embracing XR System Without Compromising on Security and Privacy' in Lucio Tommaso De Paolis, Pasquale Arpaia and Marco Sacco (eds), *Extended Reality* (Springer Nature Switzerland 2023).

¹¹⁵ *ibid.*

¹¹⁶ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJ L 151.

¹¹⁷ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). OJ L 333.

¹¹⁸ Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act). COM/2022/454 final



5.2.1. Objectives and Importance of the CSA

The Cybersecurity Act aims to create a comprehensive framework to enhance the security of ICT products, services, and processes within the European Union. This regulation is crucial for several reasons:

1. It fosters trust among consumers and businesses by ensuring consistent security measures across member states, thus reducing market fragmentation through unified cybersecurity standards.
2. The Act introduces a European cybersecurity certification framework with voluntary schemes to ensure ICT products and services meet security requirements throughout their lifecycle. Articles 46 to 50 outline the roles of ENISA and the European Commission in developing and implementing these schemes.
3. The CSA grants ENISA a permanent mandate to support member states, EU institutions, and businesses by providing expertise, promoting best practices, and facilitating cooperation. Articles 3 to 6 specify ENISA's responsibilities, which include operational coordination and cybersecurity improvements.
4. The Act imposes obligations on manufacturers to implement robust security measures during design and development phases (Article 51) and to ensure transparency about security features and vulnerabilities (Article 52).
5. Additionally, the Act supports national authorities in strengthening their cybersecurity frameworks. It emphasizes public awareness, education, and capacity building, as described in Articles 29 to 34. ENISA plays a vital role in raising public awareness, organizing cybersecurity exercises, and supporting educational initiatives.

Collectively, these provisions aim to safeguard users, promote innovation, and ensure a secure digital environment across the EU, solidifying the Cybersecurity Act as a cornerstone of the EU's cybersecurity strategy. However, the focus of the next section is on objective 4 regarding the obligations imposed on manufacturers of ICT products, service and process.



5.2.2. Obligations of Manufacturers

The Cybersecurity Act places several obligations on manufacturers of ICT products, services, and processes.¹¹⁹ These obligations are the most relevant for cybersecurity. For instance, Article 51 imposes an obligation on manufacturer to implement appropriate security measures during the design, development and production phases or the relevant technologies and ensure that the ICT products, services and processes. This includes ensuring ongoing compliance with the cybersecurity requirements throughout the lifecycle of the product.

Manufacturers must implement appropriate security measures during the design, development, and production phases of ICT products, services, and processes. These measures should ensure that products are secure by design and by default. The consortium and external partners developing the core XR components of CORTEX² must identify and implement the most suitable security measures for their various products, services, or processes. Additionally, manufacturers are obliged to make certain disclosures to the public.¹²⁰ The information that should be disclosed to the public includes:

1. Guidance and recommendations to help end-users install, apply, and maintain their products or services.
2. Contact details for reporting vulnerabilities and receiving support.
3. Known cybersecurity issues affecting their products or services.
4. The duration for which they offer security support for their products.
5. Clear descriptions of the security features and any relevant certifications they have obtained.
6. Reporting cybersecurity incidents and vulnerabilities related to their certified ICT products, services, and processes.¹²¹

It is pertinent to note that pursuant to Article 53 CSA, manufacturers are expected to collaborate with national cybersecurity certification authorities and ENISA to ensure that their products,

¹¹⁹ Article 51 – 53 CSA

¹²⁰ Article 52 CSA

¹²¹ *ibid.*



services, and processes comply with the EU cybersecurity certification schemes which are discussed below.

5.2.3. Certification Schemes

As of January 31, 2024, the European Union has introduced its first cybersecurity certification scheme, known as the European Cybersecurity Scheme on Common Criteria (EUCC),¹²² developed by ENISA. This initiative, based on the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), aims to enhance ICT security across the EU by providing a voluntary certification framework for ICT goods, services, and processes. It replaces previous national systems and establishes a single standard for cybersecurity assurance, thereby fostering a trustworthy digital market in the EU and encouraging enterprises to adhere to cybersecurity requirements.

Although the certification scheme is voluntary, adopting it plays a crucial role in improving the security and reliability of ICT products, services, and processes throughout the EU. The scheme is particularly pertinent for XR technologies, such as CORTEX², due to their integration with various IoT devices, cloud storage solutions, and other digital components.

The EUCC offers a standardized framework for assessing and certifying the cybersecurity measures of ICT products. It includes a comprehensive set of rules, technical requirements, and evaluation procedures designed to ensure that these products meet specific security standards¹²³ for XR technologies, this means that devices and services like CORTEX² can be evaluated for their security protocols and measures.

Pursuant to Article 54 of the CSA, three security levels can be achieved under the EUCC certification scheme:

¹²² Council Regulation (EU) 2024/482 of 18 June 2024 laying down rules on cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2024] OJ L200/1; 'An EU Prime! EU Adopts First Cybersecurity Certification Scheme' (ENISA) <<https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme>> accessed 23 June 2024.

¹²³ 'European Commission Launches EU Cybersecurity Certification Scheme for ICT Products | Digital Watch Observatory' (31 January 2024) <<https://dig.watch/updates/european-commission-launches-eu-cybersecurity-certification-scheme-for-ict-products>> accessed 23 June 2024



1. **Basic:** Suitable for low-risk products where the impact of a cybersecurity incident is minimal.
2. **Substantial:** Suitable for medium-risk products where the impact of a cybersecurity incident is significant but not critical.
3. **High:** Suitable for high-risk products where the impact of a cybersecurity incident is critical.

5.3. NIS2 Directive

The NIS2 Directive supersedes the initial NIS Directive, aiming to create a solid and future-oriented cybersecurity structure within the EU. This directive which came into force in January 2023, focuses on critical sectors, and imposes an obligation on essential entities to manage risks associated with network and information systems.¹²⁴ These entities must implement suitable technical organisational and operational measures, taking into account the latest cybersecurity advancements, costs, and relevant standards.¹²⁵

The directive suggests various protective measures. Furthermore, some of the protective measures proposed by the directive include; risk analysis and information system Security; incident handling; business continuity; supply chain security; system acquisition, development, and maintenance; cybersecurity risk management measures assessment; cyber hygiene and training; cryptography and encryption use; human resources security and access control; authentication and secure communication such as multi-factor or continuous authentication solutions, secured voice, video and text communications.¹²⁶ The measures can be used to support some of the security features already adopted in various aspects of CORTEX2 such as authentication and encryption.

In addition, member states are expected to transpose the NIS2 Directive by 17 October 2024, however, adopting XR technologies, such as CORTEX², in critical sectors like public administration and healthcare underscores the importance of the NIS2 Directive. This adoption activates various impending obligations, including the requirements of Article 23 of the NIS2

¹²⁴ NIS 2 Directive, Annex 1

¹²⁵ NIS 2 Directive, Art. 21(1)

¹²⁶ NIS 2 Directive, Art. 21(1)



Directive, which mandates reporting significant incidents to the competent authorities or responsible national bodies. Pursuant to the NIS2 Directive, an incident is deemed significant if it results in severe operational disruption, financial loss, or considerable damage to other parties.¹²⁷

5.4. Overview of Cyber Resilience Act Proposal

On 12 March 2024, the European Parliament approved the proposed Cyber Resilience Act (CRA). The CRA was established to enhance cybersecurity across smart and connected devices, particularly those integrating digital elements.¹²⁸ Pursuant to the CRA, "products with digital elements" broadly refers any software or hardware product along with their remote data processing solutions, and including stand-alone software or hardware components.¹²⁹

The CRA proposal lays out two sets of essential requirements for manufacturers to wit: Annex 1 section 1 and section 2 which provide for product cybersecurity requirements and vulnerability handling process requirements respectively. The CRS proposal mandates a comprehensive set of cybersecurity requirements such as secure design, protection against unauthorized access, and ensuring data integrity and availability.¹³⁰ In addition, manufacturers are required to manage vulnerabilities, perform security testing, disclose fixed vulnerabilities, and provide regular security updates.¹³¹ However, although the exclusion is not expressly stated in the CRA, it appears that the CRA is not applicable to software as a service SaaS, which is already under the purview of the NIS2 Directive.¹³² In the next section we discuss the potential applicability of the CRA proposal to CORTEX².

¹²⁷ Article 23(3)(b) NIS2 Directive; I. Lella et al., ENISA Threat Landscape 2021: April 2020 to Mid-July 2021, ENISA, 2021, cited in P. G. Chiara, "The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements," International Cybersecurity Law Review, vol. 3, pp. 255, 2022

¹²⁸ Article 3(1) CRA

¹²⁹ Article 5 CRA

¹³⁰ Articles 8 – 10 CRA

¹³¹ Article 11 CRA

¹³² Karsten Verhagen and Ellen Gielen (Houthoff), 'Cyber Resilience Act' (Houthoff, 9 April 2024) <https://www.houthoff.com/insights/news-update/cyber-resilience-act-april-2024> accessed 23 June 2024.



5.4.1. Applicability of CRA to CORTEX²

The goals of CORTEX² include providing support for XR experiences, optimizing teleconferencing tools, enabling user-friendly XR interactions, and integrating IoT devices for immersive interactions. The applicability of the CRA to CORTEX² is a complex and ongoing debate. Based on certain aspects of the design and operation of the CORTEX² framework, the CRA could indeed be applicable.

The CRA is not intended to apply to Software as a Service (SaaS) unless the solution provided qualifies as “remote data processing” as defined in Article 3(2) of the proposal. According to this definition, 'remote data processing' refers to any data processing at a distance for which the software is designed and developed by the manufacturer or under the manufacturer's responsibility. The absence of such processing would prevent the product with digital elements from performing one of its functions. In this context, remote data processing specifically refers to the use of cloud computing services to handle and process data at a distance from the local device.¹³³

The definitions explored above can be applied to CORTEX² when considering the framework's dependence on its core components. Some of the capabilities of CORTEX², such as real-time collaboration, avatar generation, environment modelling, and IoT integration, rely on remote data processing. Without this capability, it is unlikely that CORTEX² would be able to offer the intended XR experiences and telecooperation.

Additionally, the presence of specific stand-alone software modules developed or integrated into the broader CORTEX² framework further supports this functional dependence. For instance, the Mediation Gateway (Rainbow) in CORTEX², although a cloud-based service, is essential for CORTEX² to function. Therefore, the CRA proposal is an important framework to consider in the design, development, and deployment of CORTEX². However, it is pertinent to

¹³³ Baharon MR and others, 'Secure Remote Data Processing in Cloud Computing' [2013] International Journal of Computer Theory and Engineering 920



mention that open-source and non-commercial software are excluded from the CRA, and this exclusion will be discussed in the next section in connection to CORTEX².

5.4.2. Exclusions for Open-Source and Non-Commercial Software

The CRA explicitly excludes free and open-source software developed and distributed outside commercial contexts.¹³⁴ Most of the CORTEX² framework's core components will be provided under open-source licenses, with the exception of the mediation gateway, which will be the only proprietary software. For instance, an open-source module for 3D reconstruction or avatar generation could be excluded from CRA if they are not commercialised.

However, commercial activities under the CRA include charging for technical support services, managing revenue-generating software platforms, and using personal data for purposes beyond security and interoperability, such as targeted advertising or behavior analytics.¹³⁵ These activities would fall under the CRA's purview.¹³⁶ Therefore, offering subscription-based access to advanced XR features within the CORTEX² platform could also be classified as a commercial activity. Therefore, the CRA remains applicable. Since the Rainbow platform, which serves as the backbone for CORTEX², is an enterprise proprietary software, and not provided for free, complying with CRA cybersecurity requirements is essential.¹³⁷

Recommendations	<div>23. Integrate strong security protocols during the design, development, and deployment phases to ensure products are secure by design and by default.</div> <div>24. Use encryption, access control, and multi-factor authentication to protect personal data and prevent unauthorized access</div> <div>25. Pursue/encourage certification under the EUCC to ensure that the relevant</div>
------------------------	---

¹³⁴ Article 3 CRA Proposal.
¹³⁵ Recital 10, CRA.
¹³⁶ Article 4 CRA.
¹³⁷ 'About Rainbow | Alcatel-Lucent Enterprise' <<https://www.al-enterprise.com/en/rainbow/about-rainbow>> accessed 22 June 2024.



	<p>components of CORTEX² meets high security standards.</p> <p>26. Ensure continuous compliance with evolving cybersecurity standards and regulations.</p> <p>27. Establish clear protocols for incident handling, including detection, response, and reporting.</p> <p>28. Implement redundancy and backup systems to safeguard against data breaches and ensure business continuity.</p>
--	---

6. Data Governance Framework

The EU has established a comprehensive Data Governance Framework designed to foster a secure, innovative, and competitive digital economy.¹³⁸ Central to this framework is the EU Data Strategy, which aims to create a common European data space that enables easy and secure data sharing across various sectors and member states.¹³⁹ Key elements of the EU Data Strategy include:¹⁴⁰

1. **Interoperability and data disambiguation:** encouraging the use of common standards and formats to facilitate data sharing and reuse..
2. **Up-skilling and Literacy:** improving digital skills and data literacy among Europeans to ensure they can actively participate in and benefit from the data economy.
3. **Innovation and Competitiveness:** Encouraging innovation and competition by supporting start-ups and small and medium-sized enterprises (SMEs) in the data economy.

¹³⁸ European Commission. (2020). "A European strategy for data." COM(2020) 66 final

¹³⁹ *ibid.*

¹⁴⁰ *ibid*; Stec M and Grzebyk M, 'The Implementation of the Strategy Europe 2020 Objectives in European Union Countries: The Concept Analysis and Statistical Evaluation' (2018) 52 Quality & Quantity 119



The key themes identified in the EU data strategy also link back to three pivotal legal instruments: the Data Act,¹⁴¹ the Digital Services Act (DSA),¹⁴² and the Digital Markets Act (DMA). Each of these instruments plays a vital role in shaping data governance, digital services, and market dynamics, especially concerning the extensive data generated by emerging technologies such as XR platforms.

6.1. The EU Data Act

The EU legislative initiative, effective from January 11, 2024, aims to promote an open data economy by improving access to data and enhancing data sharing across multiple sectors. This includes business-to-business, business-to-government, and data from connected devices (IoT).¹⁴³ According to the EDPB and EDPS, the data act applies to a wide range of products and services, including connected objects (IoT), medical and health devices, and virtual assistants. It is important to note that the relevance of this act to the CORTEX² project lies in its integration of both IoT and virtual assistants. While CORTEX² is not the manufacturer of IoT devices as envisaged in this scenario, the Data Act's stipulations on data derived from connected devices and services do not fall under the purview of the Data act.¹⁴⁴ However, a virtual assistant is being developed under the CORTEX² project and this requires paying closer attention to the requirements of the Data Act.

As a legal instrument governing the EU digital sphere, the Data Act clarifies who can create value from data and under what conditions exploitation is permissible. These conditions are established through key provisions of the Data Act, which address various obligations such as data access and use rights;¹⁴⁵ data portability;¹⁴⁶ unfair contractual terms;¹⁴⁷ international data

¹⁴¹ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L 2854.

¹⁴² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265.

¹⁴³ Data Act, Explanatory Memorandum; D. Spajic and T. Lalova-Spinks, "The broadening of the right to data portability for IoT products: Who does the Act actually empower?" in White Paper on the Data Act Proposal: Will the Data Act Proposal actually empower?, Centre for IT & IP Law (CiTiP), KU Leuven, 2022, pp. 27-29

¹⁴⁴ Recital 15 Data Act

¹⁴⁵ Article 4 Data Act

¹⁴⁶ Article 5 Data Act

¹⁴⁷ Article 13 Data Act



transfer;¹⁴⁸ public sector access to private data, design requirements and transparency,¹⁴⁹ unlawful international governmental access and transfer;¹⁵⁰ interoperability of data processing service;¹⁵¹ technical protection measures on the unauthorised use or disclosure of data,¹⁵² among others.

For CORTEX², certain provisions are particularly salient. Enhanced data portability, as provided for in the Data Act, is of utmost relevance to the project. The Data Act extends the right to data portability to natural persons and applies to both personal and non-personal data, thereby encouraging interoperability.¹⁵³ Article 3(1) stipulates that connected products and related services must be designed to ensure that the data they generate, along with the necessary metadata for interpretation and use, are readily accessible to users. This data should be available by default in a secure, free, comprehensive, structured, commonly used, and machine-readable format.¹⁵⁴ Where relevant and technically feasible, the data should be directly accessible to the user.¹⁵⁵ CORTEX² provides open APIs and software development kits (SDKs) to facilitate interoperability with other systems and platforms, this in line with the aspirations of the Data act with regards to the right to data portability and with the interoperability and data disambiguation theme.

6.2. Digital Services package

The Digital Services Act (DSA) and the Digital Markets Act (DMA) collectively establish a comprehensive regulatory framework applicable across the European Union. These legislative measures aim to achieve two primary objectives.¹⁵⁶ First, the DSA seeks to create a safer digital environment by safeguarding the fundamental rights of all users of digital services. Second,

¹⁴⁸ Article 28 Data Act

¹⁴⁹ Article 3(1) Data Act

¹⁵⁰ Article 32 Data Act

¹⁵¹ Article 33 – 35 Data Act

¹⁵² Article 11 Data Act

¹⁵³ S. F. Ennis and B. Evans, "Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence." Rochester, NY, Mar. 22, 2023. doi: 10.2139/ssrn.4395183; A. Stenzel and I. Waichman, "Supply-chain data sharing for scope 3 emissions," npj Clim. Action, vol. 2, no. 1, Art. no. 1, Mar. 2023, doi: 10.1038/s44168-023-00032-x.

¹⁵⁴ Article 3(1) Data Act.

¹⁵⁵ *ibid.*

¹⁵⁶ European Commission, 'Digital Services Act Package' (European Commission, 2024) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 28 June 2024.



they strive to establish a level playing field that encourages innovation, growth, and competitiveness within the European Single Market and globally. By addressing both user protection and market fairness, the DSA and DMA represent significant steps towards a more secure and dynamic digital economy in the EU.

6.2.1. Digital Services Act

The DSA aims to ensure the proper functioning of the EU internal market for intermediary services by establishing harmonised rules that create a safe, predictable, and trusted online environment, thereby facilitating innovation and protecting fundamental rights, including consumer protection.¹⁵⁷ It sets out specific provisions for conditional liability exemptions for intermediary service providers, mandates due diligence obligations for certain categories of these providers, and outlines the implementation and enforcement mechanisms, including cooperation and coordination between competent authorities.¹⁵⁸ The primary focus of the DSA is on harmful and illegal goods, services, and online content, which may impact how XR platforms handle illegal and harmful content, and targeted advertisements.¹⁵⁹

The relevance for CORTEX² stems from the intermediary services identified in the project. Recital 29 of the DSA indicates that "intermediary services span a wide range of economic activities which take place online and that develop continually to provide for the swift, safe, and secure transmission of information, ensuring convenience for all participants of the online ecosystem." This wide range of economic activities includes mere conduit, caching and hosting services.¹⁶⁰ For instance, the Mediation Gateway in CORTEX² can be considered a "mere conduit" service under the DSA because it facilitates the transmission of various data among users without initiating the transmission, selecting the receiver, or modifying the information contained in the transmission.¹⁶¹

¹⁵⁷ Article 1(1) DSA.

¹⁵⁸ Article 1(2) DSA

¹⁵⁹ Hine E and others, 'Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations' <<https://papers.ssrn.com/abstract=4585963>> accessed 28 June 2024.

¹⁶⁰ Article 4, 5 & 6 DSA

¹⁶¹ Article 4(1)(a) DSA



XR poses heightened risks to children and other vulnerable and marginalised persons.¹⁶² These risks can arise from using XR platforms in public-facing sectors like education, where there could be interaction with minors. Pursuant to Article 28, providers of online platforms accessible to minors must put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security for minors. To achieve this protection, intermediary services in the XR ecosystem should assess risks associated with the safety of XR users and the misuse of such platforms, as highlighted in Recital 80 of the DSA.¹⁶³

The DSA mandates providers of very large online platforms to assess four categories of risks: (1) dissemination of illegal content, (2) impact on fundamental rights, (3) effects on democratic processes and public security, and (4) risks to physical and mental well-being. It should be noted that at the time of this analysis, the DSA does not apply to providers in CORTEX² because there is a threshold to qualify and be designated as a Very Large Online Platform (VLOP). However, it is pertinent to take a proactive approach to mitigate risks posed by XR platforms to facilitate the safety and well-being of users, especially vulnerable ones.

6.2.2. Digital Markets Act

The DMA is geared towards regulating market behaviour and anti-monopoly control to create fair competition for all digital companies by establishing higher standards of transparency and responsibility, especially for large online platform providers called "gatekeepers."¹⁶⁴ Although the actors in CORTEX² are not designated gatekeepers for the purposes of this analysis, some requirements need to be evaluated to ensure that CORTEX² addresses concerns related to core platform services such as the conversational agent (virtual assistant) and the cloud computing services required for CORTEX² to function.¹⁶⁵

¹⁶² Pahi S and Schroeder C, 'Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy Is Several of Them' (2023) 4 Notre Dame Journal on Emerging Technologies (JET) 1

¹⁶³ Franklyn Ohai and Maja Nisevic, Legal challenges of Cooperative Real-Time Extended reality: insights from the EU, 9th International XR-Metaverse Conference, Busan, May 2024.

¹⁶⁴ Yadong C, 'Special Reports on the Development of Artificial Intelligence Rule of Law' in Cui Yadong (ed), Blue Book on AI and Rule of Law in the World (2022) (Springer Nature 2024) <https://doi.org/10.1007/978-981-97-1060-7_9> accessed 28 June 2024

¹⁶⁵ Article 2 DMA.



Pursuant to the DMA, a "virtual assistant" is defined as software that processes demands, tasks, or questions, including those based on audio, visual, written input, gestures, or motions, and provides access to other services or controls connected physical devices.¹⁶⁶ Therefore, the conversational agent in CORTEX² will benefit from meeting the requirements of the DMA, even without an official gatekeeper designation.

Pursuant to Article 5, CORTEX² must implement measures to prevent the processing of personal data from third-party services and prevent the combination and cross-use of personal data from core platform services provided by CORTEX² or third-party services.

Article 6 Ensures fair competition and data privacy by requiring gatekeepers to allow easy removal of software, enable third-party app use, and provide data portability and access to users and business partners. This provision aligns with the interoperability and portability themes emphasized in this deliverable and the steps already taken by the project.

Recommendations

29. Use common standards and formats to facilitate seamless data sharing and re-use across different systems and sectors.
30. Align data sharing practices with the EU Data Act, focusing on business-to-business (B2B) and business-to-government (B2G) data sharing.
31. Implement measures to prevent the dissemination of harmful and illegal content on CORTEX² platforms when the need arises.
32. Ensure high levels of privacy, safety, and security for all users, especially minors, as required by the DSA.
33. Meet fair competition and data privacy requirements, even if not designated as a gatekeeper.

¹⁶⁶ Article 2(12) DMA.



	34. Facilitate easy integration and removal of third party software and provide data portability and access to business users.
--	--

7. Conclusion

The CORTEX² project marks a significant leap forward in integrating advanced AI and XR technologies into various industrial and corporate settings. This deliverable provides a comprehensive analysis of the ethical, legal, and technical frameworks supporting the development and deployment of the CORTEX² platform, offering 34 targeted recommendations. While many of these recommendations are grounded in existing measures, they offer bespoke guidance tailored to the unique context of CORTEX² and similar technologies.

A key highlight of this analysis is the project's adherence to GDPR principles, ensuring robust data protection and user privacy. The project demonstrates compliance through its secure-by-design architecture, which incorporates data encryption and stringent access controls. Additionally, the project's focus on data minimization, accuracy, and storage limitation ensures that only essential data is processed and retained, thereby safeguarding individual rights and freedoms.

The exploration of the AI Act clarifies the roles and responsibilities of various actors within the CORTEX² ecosystem. By clearly defining entities such as providers, deployers, and distributors, this deliverable ensures that all stakeholders are aware of their obligations. Ethical considerations have been meticulously addressed, particularly in terms of human autonomy, harm prevention, fairness, and explicability. The deliverable integrates guidelines from the High-Level Expert Group on AI (HLEG), ensuring that AI components are developed and utilized in ways that respect human dignity and prevent misuse.

Moreover, the analysis emphasizes the importance of AI literacy among users and operators. By prioritizing education and training, CORTEX² aims to cultivate a technically proficient user base capable of effectively utilising the platform and mitigating potential risks. The efforts to



foster accessibility and inclusivity in CORTEX² ensures that the solutions developed within the project are user-friendly for diverse groups, including individuals with disabilities. Continuous stakeholder engagement and iterative testing are impending to further enhance accessibility and inclusivity.

In conclusion, the CORTEX² project demonstrates a comprehensive approach to adhering to ethical, legal, and technical standards. By addressing the complexities of XR and the enabling technologies in CORTEX², this deliverable not only advances the legal and ethical discourse but also sets a benchmark for responsible and inclusive technology development.



Bibliography

Legislation

- Council Regulation (EU) 2024/482 of 18 June 2024 laying down rules on cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2024] OJ L200/1
- Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act). COM/2022/454 final
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJ L 151
- Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277
- Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L 2854
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 173/1

Case Law

- Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.
- CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 May 2009.



- Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECJ Joined Cases C293/12 and C594/12

Official Documents

- Council of the European Union, 'AIA – CZ – General Approach' (25 November 2022) ST 12149 2022 INIT <https://data.consilium.europa.eu/doc/document/ST-12149-2022-INIT/en/pdf>
- High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (2019) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 accessed 28 June 2024
- European Commission, 'A European Strategy for Data' COM(2020) 66 final, 2020

Other Sources

- A Aloisi and E Gramano, 'Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context Automation, Artificial Intelligence, & Labor Law' (2019) 41 Comparative Labor Law & Policy Journal 95
- An EU Prime! EU Adopts First Cybersecurity Certification Scheme (ENISA) <https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme>
- AP y Madrid and C Wright, Trustworthy AI Alone Is Not Enough (ESIC 2023)
- Arto Laitinen and Otto Sahlgren, 'AI Systems and Respect for Human Autonomy' (2021) 4 Frontiers in Artificial Intelligence <https://www.frontiersin.org/articles/10.3389/frai.2021.705164>
- D Spajic and T Lalova-Spinks, 'The Broadening of the Right to Data Portability for IoT Products: Who Does the Act Actually Empower?' in White Paper on the Data Act Proposal: Will the Data Act Proposal Actually Empower?, Centre for IT & IP Law (CiTiP), KU Leuven, 2022
- Diane Hosfelt, 'Making Ethical Decisions for the Immersive Web' (arXiv, 14 May 2019) <https://doi.org/10.48550/arXiv.1905.06995>
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) [2022] OJ L333
- E Hine and others, 'Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations' <https://papers.ssrn.com/abstract=4585963>



- European Commission Launches EU Cybersecurity Certification Scheme for ICT Products (Digital Watch Observatory, 31 January 2024) <https://dig.watch/updates/european-commission-launches-eu-cybersecurity-certification-scheme-for-ict-products> accessed 23 June 2024
- European Commission, 'Digital Services Act Package' (European Commission, 2024) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 28 June 2024
- F De Felice and others, 'Physical and Digital Worlds: Implications and Opportunities of the Metaverse' (2023) 217 Procedia Computer Science 1744
- Franklyn Ohai and Maja Nisevic, 'Legal Challenges of Cooperative Real-Time Extended Reality: Insights from the EU', 9th International XR-Metaverse Conference, Busan, May 2024
- IB Adhanom, P MacNeilage and E Folmer, 'Eye Tracking in Virtual Reality: A Broad Review of Applications and Challenges' (2023) 27 Virtual Reality 1481
- J Greene, 'Ethical Design Approaches for Workplace Augmented Reality' (2023) 10 Communications Design Quarterly Review 16
- James H Moor, 'Why We Need Better Ethics for Emerging Technologies' (2005) 7 Ethics and Information Technology 111
- K Smit, M Zoet and JV Meerten, 'A Review of AI Principles in Practice' presented at the Pacific Asia Conference on Information Systems, 2020
- Karsten Verhagen and Ellen Gielen, 'Cyber Resilience Act' (Houthoff, 9 April 2024) <https://www.houthoff.com/insights/news-update/cyber-resilience-act-april-2024> accessed 23 June 2024
- Kerem Gülen, 'OpenAI Used YouTube Videos to Train AI, Report Claims' (Dataconomy, 8 April 2024) <https://dataconomy.com/2024/04/08/openai-used-youtube-videos-to-train-ai-report-claims/> accessed 21 June 2024
- Lella et al., 'ENISA Threat Landscape 2021: April 2020 to Mid-July 2021', ENISA, 2021, cited in PG Chiara, 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements' (2022) 3 International Cybersecurity Law Review 255
- Meenaakshisundaram K, 'The Ethics of Extended Realities: Insights from a Systematic Literature Review' (2023)



- Melvin Abraham and others, 'Implications of XR on Privacy, Security and Behaviour: Insights from Experts', Nordic Human-Computer Interaction Conference (Association for Computing Machinery 2022) <https://dl.acm.org/doi/10.1145/3546155.3546691>
- MR Baharon and others, 'Secure Remote Data Processing in Cloud Computing' [2013] International Journal of Computer Theory and Engineering 920
- Nathalie A Smuha, 'The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence' (2019) <https://papers.ssrn.com/abstract=3443537> accessed 2 June 2024
- Osman Koroglu, 'Ethics in AI, XR and Digitalization: A Systematic Literature Review' in Book of Proceedings
- Pahi S and Schroeder C, 'Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy Is Several of Them' (2023) 4 Notre Dame Journal on Emerging Technologies (JET) 1
- R Acheampong and others, 'Embracing XR System without Compromising on Security and Privacy' in Lucio Tommaso De Paolis, Pasquale Arpaia and Marco Sacco (eds), Extended Reality (Springer Nature Switzerland 2023)
- R Acheampong, TC Balan, D-M Popovici, and A Rekeraho, 'Embracing XR System Without Compromising on Security and Privacy' in L T De Paolis, P Arpaia, and M Sacco (eds), Extended Reality, Lecture Notes in Computer Science (Springer Nature Switzerland 2023) doi: 10.1007/978-3-031-43401-3_7
- S Baker and others, 'Interrogating Social Virtual Reality as a Communication Medium for Older Adults' (2019) 3 Proc ACM Hum-Comput Interact 149:1
- S Schöbel, A Schmitt, D Benner, M Saqr, A Janson, and JM Leimeister, 'Charting the Evolution and Future of Conversational Agents: A Research Agenda Along Five Waves and New Frontiers' (2023) Inf Syst Front doi: 10.1007/s10796-023-10375-9
- SF Ennis and B Evans, 'Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence' (2023) <https://doi.org/10.2139/ssrn.4395183>
- Stec M and Grzebyk M, 'The Implementation of the Strategy Europe 2020 Objectives in European Union Countries: The Concept Analysis and Statistical Evaluation' (2018) 52 Quality & Quantity 119
- Stenzel and I Waichman, 'Supply-chain data sharing for scope 3 emissions' (2023) 2(1) npj Clim Action 1 <https://www.nature.com/articles/s44168-023-00032-x>



- Tao H Barrios, V Pérez and Y Guerra Post, 'Artificial Intelligence and Education: Challenges and Disadvantages for the Teacher' (2019) 72 Arctic Medical Research 30
- Triguero I and others, 'General Purpose Artificial Intelligence Systems (GPAIS): Properties, Definition, Taxonomy, Societal Implications and Responsible Governance' (2024) 103 Information Fusion 102135
- Vallor S, Raicu I and Green B, 'Technology and Engineering Practice: Ethical Lenses to Look Through' [2020] Markkula Center website
- Vallor, Raicu and Green, 'Technology and Engineering Practice: Ethical Lenses to Look Through' [2020] Markkula Center website p18
- van der Krabben, E., Kooij, H.-J., Raaphorst, K., & Hoekman, R., 'The Impact of the Built Environment and Social Environment on Physical Activity: A Scoping Review' (2023) International Journal of Environmental Research and Public Health
- Walter Y, 'Embracing the Future of Artificial Intelligence in the Classroom: The Relevance of AI Literacy, Prompt Engineering, and Critical Thinking in Modern Education' (2024) 21 International Journal of Educational Technology in Higher Education 15
- Windelband L, 'Artificial Intelligence and Assistance Systems for Technical Vocational Education and Training – Opportunities and Risks' in Alexandra Shajek and Ernst Andreas Hartmann (eds), New Digital Work: Digital Sovereignty at the Workplace (Springer International Publishing 2023) https://doi.org/10.1007/978-3-031-26490-0_12
- Yadong C, 'Special Reports on the Development of Artificial Intelligence Rule of Law' in Cui Yadong (ed), Blue Book on AI and Rule of Law in the World (Springer Nature 2024) https://doi.org/10.1007/978-981-97-1060-7_9
- Y-W Chow and others, 'Visualization and Cybersecurity in the Metaverse: A Survey' (2023) 9 Journal of Imaging 11