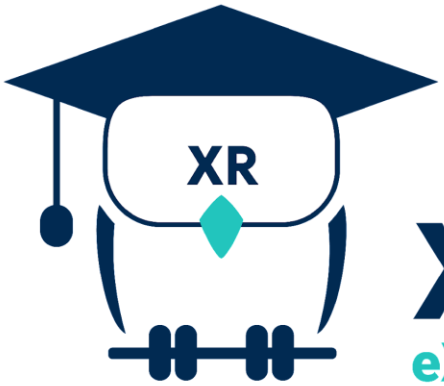
Horizon Innovation Action
HORIZON-CL4-2022-HUMAN-01-19



XR4ED
eXtended Reality for EDucation

D2.1
Data Protection Impact Assessment Methodology

DISCLAIMER
This document is issued within the frame and for the purpose of the XR4ED project. This project has received funding from the European Union's Horizon Europe Framework Programme under Grant Agreement No. 1010931159. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission. The dissemination of this document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission. This document and its content are the property of the XR4ED consortium. The content of all or parts of this document can be used and distributed provided that the XR4ED project and the document are properly referenced. Each XR4ED partner may use this document in conformity with the XR4ED Consortium Grant Agreement provisions.

Funded by
the European Union

XR4ED Project Profile

Project title	eXtended Reality for EDucation
Project acronym	XR4ED
Grant agreement No.	101093159
Start date of project	1 January 2023
Duration of project	36 months
Project website	http://www.XR4ED.eu

Partners

CYENS CENTRE OF EXCELLENCE	CYENS	RESEARCH	CYPRUS
konnektable TECHNOLOGIES	KONNEKTABLE	SME	IRELAND
21 Sci science 27 Co communication	SciCo	SME	GREECE
F6S	F6S	SME	IRELAND
INFINITIVITY DESIGN LABS	Infinity Design Labs	SME	FRANCE
KAINOTOMIA	KAINOTOMIA	SME	GREECE
NUROGAMES	NUROGAMES	SME	GERMANY
VASS	VASS Company	INDUSTRY	Luxemburg
SIMAVI	Software Imagination & Vision SRL	SME	ROMANIA
UPC	Universitat Politecnica de Catalunya	RESEARCH	SPAIN
CELLOCK	CELLOCK	SME	CYPRUS

Document information

Related work package	WP2	
Document reference	D2.1	
Related deliverables		
Type		DEM - Demonstrator, Pilot, Prototype
		DMP - Data Management Plan
	✓	R - Document, Report
Status	Final	
Version	4	
Due date	31/10/2023	
Submission date	30/10/2023	
Lead partner	KAINOTOMIA	
Contributing partners	CYENS, IDL, NUROGAMES, SIMAVI	
Reviewers	Athina Papandreou (KAINOTOMIA),	
Keywords	Data Protection, Data Protection Impact Assessment, Methodology, XR	

Dissemination level	
✓	PU: Public
	SEN: Sensitive

List of contributors	
Name	Partner (short name)
Athina Papandreou	KAIN
Alkis Nicolaides	CYENS
Fotis Liarokapis	CYENS

Revision History

Document History			
Version	Date	Change editors	Changes
1.0	28/09/2023	Athina Papandreou (KAIN)	Initial version of the document
2.0	25/10/2023	Athina Papandreou (KAIN)	Second version of the document
3.0	30/10/2023	Athina Papandreou (KAIN)	Final version of the document
4.0	30/10/2023	Alkis Nicolaides, Fotis Liarokapis (CYENS)	Formatting changes, additions and final checking

Quality control		
Role	Partner (short name)	Approval date
Deliverable leader	KAIN	30/10/2023
Quality manager	CLK	30/10/2023
Project coordinator	CYENS	30/10/2023

Table of contents

XR4ED Project Profile 2
Partners 3
Document information 4
Revision History 5
List of Figures 8
List of Tables 8
List of acronyms 9
Executive summary 10
1. INTRODUCTION AND THEORY 11
1.1. ETHICS IN XR FOR EDUCATION 11
1.1.1 INCLUSIVE EDUCATION 12
2.1.1 ACCESSIBILITY 13
3.1.1 PERSONAL DATA 13
2. PURPOSE-OBJECT OF THE PRESENT STUDY 20
2.1. METHODOLOGY 20
2.2. THE METHOD FOLLOWED FOR THE IDENTIFICATION AND ANALYSIS OF RISKS 21
3. IMPLEMENTATION OF A DATA PROTECTION IMPACT ASSESSMENT STUDY ON THE XR4ED PLATFORM 23
3.1. ASSESSMENT OF THE MEASURES GUARANTEEING THE PROPORTIONALITY AND NECESSITY OF THE PROCESSING IN XR4ED 23
3.2. OVERVIEW OF THE MAIN PARAMETERS OF THE TREATMENT 24
3.3. PERSONAL DATA - RECIPIENTS 25
3.4. THE RIGHTS OF DATA SUBJECTS 29
3.5. PROPORTIONALITY STUDY 31
3.6. STUDY OF POTENTIAL CHALLENGES IN RELATION TO THE RIGHTS OF STUDENTS AND EDUCATORS 32
3.6.1. CHALLENGES-RISKS IN RELATION TO RIGHTS AND TECHNICAL ISSUES 32
3.7. TECHNICAL CHALLENGES IN RELATION TO THE DEVELOPMENT OF XR TECHNOLOGIES 35
3.8. STUDY OF SAFETY MEASURES 35

3.8.1. EXISTING SECURITY MEASURES 35
3.9. EXISTING MEASURES TO MEET ETHICAL REQUIREMENTS 37
3.9.1. IDENTIFICATION AND ASSESSMENT OF RISKS RELATED TO THE PROTECTION OF PERSONAL DATA 37
3.9.2. RISK OF UNLAWFUL ACCESS TO PERSONAL DATA COLLECTED BY THE PLATFORM 38
3.9.3. RISK OF UNLAWFUL ACCESS TO PERSONAL DATA DURING TRANSMISSION 41
3.9.4. RISK OF CHANGE OF PERSONAL DATA 43
3.9.5. RISK OF LOSS OF PERSONAL DATA 45
4. CONCLUSIONS 48

List of Figures

Figure 1 – Definition of XR (https://xr4europe.eu/whatisxr/) 11

List of Tables

Table 1: Personal Data - Recipients 28
Table 2: Rights of the Data Subjects 30
Table 3: Risk Of Unlawful Access To Personal Data Collected By The Platform 40
Table 4: Risk Of Unlawful Access To Personal Data During Transmission 42
Table 5: Risk Of Unlawful Access To Personal Data During Transmission 44
Table 6: Risk Of Loss Of Personal Data 46
Table 7: Likert Scale For Measuring The Impact On Personal Data 47
Table 8: Likert scale for capturing the effects on privacy 47

List of acronyms

Acronym	Description
XR4ED	Extended Reality for Education
XR	Extended Reality
AR	Augmented Reality
VR	Virtual Reality
MR	Mixed Reality
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
FAIR	Findable, Accessible, Interoperable and Reusable

Executive summary

The deliverable entitled "D2.1 Data Protection Impact Assessment Methodology" provides a comprehensive analysis of the data protection and ethical considerations associated with the XR4ED platform. This assessment focuses on the use of Extended Reality (XR) technologies in education, highlighting the platform's commitment to safeguarding the rights and privacy of students and educators.

The deliverable begins by emphasizing the importance of considering the proportionality principle in relation to using XR technologies for education. It underlines the effectiveness of XR technologies in providing education while respecting personal data protection and ethical principles. The adoption of Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) applications within the XR platform facilitates a seamless and immersive educational experience, particularly beneficial for students with disabilities.

A critical concern addressed is the potential impact on the free development of users' personalities due to the digitization of educational processes and data collection. The deliverable outlines the XR4ED platform's design to uphold collaborative learning practices and provide users with the flexibility to control their data transmission.

Privacy risks associated with data processing through modern technologies are discussed, highlighting the platform's commitment to data minimization, security, and transparency. Academic freedom for Educators and the prevention of third-party data collection are integral aspects of the XR4ED platform's ethical framework.

The deliverable also identifies several technical challenges associated with XR technologies, emphasizing the need for coordination between hardware and software components. It acknowledges resource constraints but maintains that the platform offers appropriate tools and resources to mitigate these challenges.

Detailed security measures, ethical considerations, and risk assessments are presented, encompassing the protection of personal data and adherence to privacy regulations. The deliverable provides tables and Likert scales to measure the impact on personal data and privacy.

1. INTRODUCTION AND THEORY

1.1. ETHICS IN XR FOR EDUCATION

XR is a general term that includes VR, AR and MR.

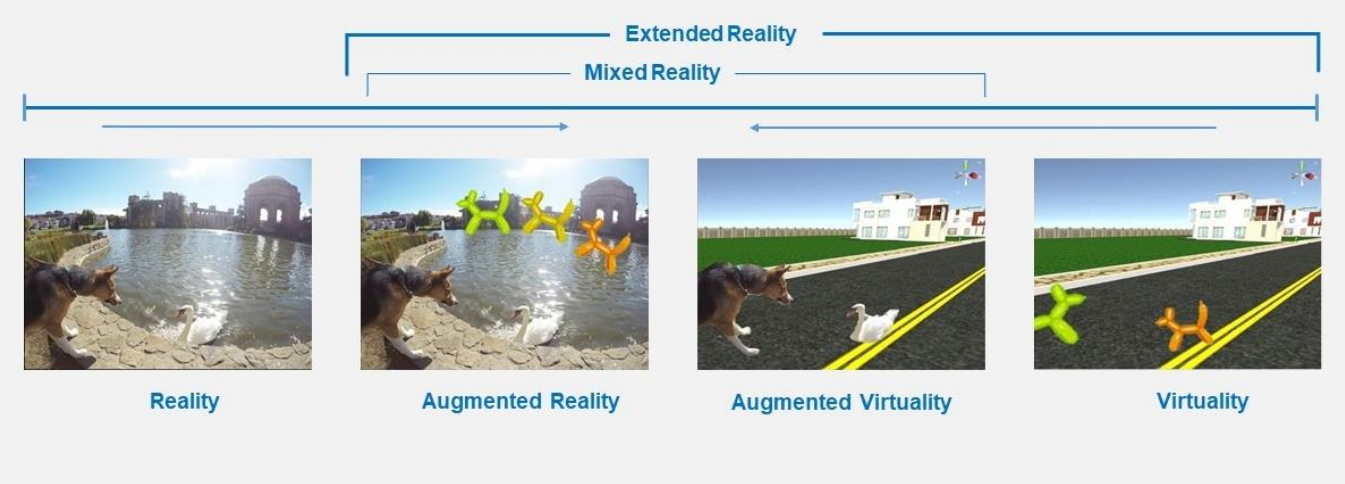


Figure 1 – Definition of XR (https://xr4europe.eu/whatisxr/)

The use of XR in education offers a unique learning experience that can be tailored to each individual student as it provides a more interactive and engaging experience, while at the same time helping students better understand complex concepts, improve their skills in a safe and controlled environment, and retain knowledge through more hands-on learning techniques (Frąckiewicz, 2023).

In any case, however, the use of XR in education poses specific ethical challenges mainly due to the processing of large volumes of data and it therefore becomes clear that it is necessary to ensure that students and Educators respectively understand the potential of XR and big data in education, while being aware of the risks involved. Therefore, certain ethical guidelines regarding the use of XR technology and data in education should be applied to ensure a safe and fair learning experience.

As the values of the European Union are common to all EU countries, the core values of tolerance, justice, solidarity and non-discrimination prevail in all European countries (Aims and Values, n.d.).

In the field of education, and by extension in education with XR technology, emphasis must be placed on respect for the individual, knowledge, democratic principles, quality of research and academic freedom, and therefore it becomes necessary for XR system providers to comply with ethical requirements.

The basic principles to be followed when using an XR training system are the following:

- Education must be conducted with full respect for scientific truth, academic freedom, the biological and intellectual integrity of the human person, human dignity, intellectual property and personal data.
- Diversity, non-discrimination, and fairness, including accessibility, universal design, avoidance of unfair bias and stakeholder participation. In particular, any discrimination of stakeholders should be avoided irrespective of ethnicity, race, gender, sexual orientation, gender identity and/or expression, social origin, language, religion, physical ability, age, level of education, and socio-economic circumstances.
- Full transparency on the methods and features of the training platform. Instructions and information should be accessible and presented in a clear way to the users of the platform.
- Protection and preservation of the natural, social, and cultural environment.
- Respect for privacy and personal data and in particular storage of data in a secure location, compliance with GDPR, informing users about the collection of their personal data and the purpose of their processing.
- Adequate security to protect user data.
- Obligation of written informing and written consent of the participating parties.

1.1.1 INCLUSIVE EDUCATION

Inclusive education is defined as the process of providing equal learning opportunities for all learners without exception. Special education aims, through an individualised approach, to address the particularities of pupils who have been categorised as having special needs (Angelides et al., 2006). Special education concerns only those pupils who may be attending special school units, such as special schools, special classes or integration classes in mainstream schools, and focuses on their integration and inclusion in the school environment and society as a whole.

Inclusive education mainly promotes the inclusion of pupils with special needs in the sense of whole education, i.e., an education that includes all pupils (formal and non-formal) and is interested in the participation of all in school life. More specifically, inclusion does not focus on individual issues but takes as its principle that the individual is embedded in a social and learning environment and that any difficulties need to be addressed as an integral part of this context (Loreman, 2017).

An important practice to promote inclusive education involves adapting instruction to meet the needs of all students. For the educator to be able to meet the needs of all students, it is therefore important to

adapt teaching accordingly and to differentiate teaching objectives to address each student individually. It is essential that teaching is personalised, while providing group activities in which pupils work together, exchange views and interact with each other (Booth, 2011).

2.1.1 ACCESSIBILITY

The inclusion of people with disabilities and other excluded groups in education has been a central objective of education policy in several systems.

As XR technology offers an alternative way of visualising content, it provides accessibility and equal opportunities in education. This is a major benefit for people with disabilities as it enables them to lead productive lives and get an education. In particular, sensory loss affects the way a person reads, is informed and communicates in general, however, through XR systems, people with disabilities will be able to rely on their other senses and use information channels through their sight, sound and touch (Basdekis, 2013).

3.1.1 PERSONAL DATA

A. LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA

As early as the 28th of January 1981, the European Convention "for the Protection of Individuals with Regard to Automatic Processing of Personal Data" (Convention 108) was adopted, followed by a series of Community regulations.

On the 27th of April 2016, the General Data Protection Regulation (Regulation 2016/679) of the European Parliament and the European Council was adopted, which entered into force on the 25th of May 2018. This Regulation was based on the EU Directive 95/46 and is the legal instrument that determines the "level of protection" of the right to the protection of personal data, and which in certain cases and under certain conditions leaves, to the Member States a discretion to adopt more specific rules, within the framework of "flexibility clauses" it contains.

The substantive scope of the Regulation is set out in Article 2 of the GDPR, as well as in Directive 95/46. In particular, the Regulation applies to the fully or partly automated processing of personal data as well as to the non-automated processing of such data which are or are to be included in a filing system, i.e., a structured set of personal data which are accessible based on specific criteria (Art. 2(1), Art. 4(6) GDPR) (Besemer & Newton, 2020).

B. CONCEPT OF PERSONAL DATA

The definition of "personal data" is reflected in Article 4 paragraph 1 of the GDPR according to which it is “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

The above definition shows that the concept of personal data is broad. Personal data means any information about a person from the simplest information such as their full name, their e-mail address, their posts on social media, up to the most "sensitive" ones, which may be their sexual preferences.

The basic element of the personal data is its connection with a specific person so that the identity of the latter can be established either directly (by reference to their name) or indirectly (by "photographing" them, such as by reference not to their name but to their office, ID number, Social Security Number, VAT number), i.e. by combining additional information that characterises their status in terms of physical, biological, psychological, economic, cultural, political or social status (Kennedy, 2019).

C. PROCESSING OF PERSONAL DATA

The concept of processing personal data is contained in Article 4 paragraph 2 of the DDPR. According to this definition, which includes an extensive but indicative list of operations constituting the processing of personal data, the concept of processing includes the collection, recording, organisation, structuring,

storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, restriction, erasure and destruction (Kanellos, 2023).

D. LAWFULNESS OF THE PROCESSING

The principle of legality is enshrined in Article 5 paragraph 1a of GDPR and is specified in the provisions of Articles 6 et seq. For processing to be lawful, in addition to the general principles of Article 5 of the GDPR, the processing must also be based on one of the conditions set out in Article 6 of the GDPR. Therefore, according to this provision, which also corresponds to the provision of Article 7 of Directive 95/46, the processing is lawful if at least one of the following conditions is met:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

It is noted that the above legal bases for the processing of personal data, pursuant to Article 6 paragraph 1 are exclusive and not indicative (Besemer & Newton, 2020), while they are all equal and none of them is superior to the others.

E. PRINCIPLES OF PROCESSING OF PERSONAL DATA

According to Article 5 of GDPR, for the processing of personal data (both simple and special categories) to be lawful, the processing must be governed by certain principles. These are:

1. **The 'lawfulness, fairness and transparency' principle**, which is a fundamental principle governing the processing of personal data, states that personal data must be processed lawfully and fairly in a transparent manner in relation to the data subject (Art.5(1) GDPR).
2. **The 'purpose limitation' principle,** according to which personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes
3. **The 'data minimisation' principle (**as a manifestation of the proportionality principle), according to which data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Compliance with the principle of minimisation is achieved by taking technical and organisational measures and in particular by implementing the anonymisation or pseudonymisation of personal data.
4. **The 'accuracy' principle,** according to which personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. **The 'storage limitation' principle,** according to which personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

6. **The 'integrity and confidentiality' principle**, according to which data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. **The 'accountability' principle,** whereby the controller is responsible and must be able to demonstrate its compliance with the principles referred to in paragraph 1 of Article 5 of the GDPR before supervisory authorities and the courts.

Processing of simple data

For the processing of simple personal data to be legal, in addition to the aforementioned general principles of Article 5 of the GDPR, some of the conditions of Article 6, paragraph 1 of the GDPR must also be established. The concept of personal data processing is included in Article 4 paragraph 2 of the GDPR. According to this definition, which includes an extensive but indicative list of acts that constitute the processing of personal data, the concept of processing includes collection, registration, organization, structure, storage, adaptation, alteration, retrieval, search information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion and destruction.

Processing of special category data

In principle, 'special category data' means personal data which are by nature particularly sensitive in relation to fundamental rights and freedoms and which require special protection, as the context in which they are processed could pose a significant risk to the fundamental rights and freedoms of the individual (Kalampouka Giannopoulou, 2020). These data relate to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric information for the purpose of positive identification of a person or data, an individual's sex life or sexual orientation, and health, such as information on physical, mental or spiritual condition (present, past or future), drug or alcohol abuse, disability or impairment, or medication. The term 'personal health data' is broader than the term 'medical data', since the former are also held by persons who do not have the status of a doctor (e.g., physiotherapists, speech and language therapists, psychologists).

Regarding the processing of special category data, it is in principle prohibited because such personal data should not be processed unless the processing is permitted in specific cases or in the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements to which such processing is subject, the general principles and other rules of the GDPR should apply, as regards the conditions for lawful processing (Process of personal data lawfully, n.d.). Article 9 paragraph 2 of the GDPR provides, inter alia, that the processing of special category data is permitted in certain cases, namely: where the data subject has given their explicit consent to the processing, the processing is necessary for the performance of obligations of the controller or the data subject in the field of labour law and social security and social protection law, for the protection of the vital interests of the data subject or of another natural person, for the protection of the data subject's vital interests or for the protection of the data subject's interests.

F. THE RIGHTS OF THE DATA SUBJECT

Right to information and transparency (Articles 12-14 GDPR):

Regarding the exercise of the data subject's rights, the provision of Article 12 of the GDPR is fundamental. In principle, it provides for the obligation of the controller to take appropriate technical and organisational measures to satisfy the data subject's right to information and access, as well as the rights of erasure, rectification, opposition, portability and to notify them of a possible personal data breach, in accordance with Article 34 of the GDPR. The relevant information shall be provided in a concise, transparent, intelligible and easily accessible form, using simple and clear wording, particularly when the information is addressed to children (Milkaite & Lievens, 2019).

Right of access (Article 15 of the GDPR):

The data subject has the right to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed.

Right to rectification (Article 16 of the GDPR):

Natural persons - data subjects - have the right to request the rectification of their data where it is inaccurate or the completion of data where it is incomplete.

Right to erasure-Right to be forgotten (Article 17 of the GDPR):

The data subject has the right to request the erasure of personal data concerning them, if they no longer wish those data to be processed, if there is no legitimate reason for the controller to hold them and if the data were processed unlawfully. In particular, the data subject may withdraw the consent on which the processing is based, in which case the data must be erased.

Right to restriction of processing (Article 18 GDPR):

Data subjects have the right to request the restriction of the processing of their data where their accuracy is contested, the processing is unlawful, the data are no longer needed by the controller or there are objections to automated processing.

Right to data portability (Article 20 GDPR):

Data subjects have the right to receive personal data relating to them which have been processed by a controller in a structured, commonly used and machine-readable format and the right to transmit those data to another controller without objection from the original controller. Where technically feasible, they may request the direct transfer of their data from one controller to another.

Right to object (Article 21 of the GDPR):

The data subject shall have the right to object, at any time and on grounds relating to his or her situation, to the processing of personal data concerning him or her, including profiling under those provisions.

Right to automated individual decision-making, including profiling (Article 22 GDPR):

The data subject shall have the right to object where a decision concerning him or her is based solely on automated processing, including profiling, and that decision produces legal effects or significantly affects him or her.

2. PURPOSE-OBJECT OF THE PRESENT STUDY

Regulation 2016/679 (GDPR) introduces the concept of an impact assessment regarding the protection of personal data (PIA). In particular, this process is designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons posed by the processing of personal data by evaluating them and defining measures to address them.

Therefore, the primary purpose is to ensure and demonstrate that the processing of personal data when using the XR4ED platform will be carried out in accordance with the fundamental principles for the protection of personal data, as they are founded in Article 5 GDPR. At the same time, through the identification and further evaluation of the risks and consequently through the determination of measures to address them, this study becomes an important tool for fulfilling the obligation of accountability, for the Processor, in addition to compliance itself according to the specifications of GDPR, to be able to demonstrate that appropriate measures have been taken to achieve this (compliance).

Furthermore, it becomes necessary to consider the application of ethical standards to the educational process and the conduct of scientific research to be carried out in the context of the operation of the XR4ED platform, in order to ensure that the provision of education using XR technology is safe and is developed and used in accordance with the obligations arising from fundamental rights.

2.1. METHODOLOGY

This study sets out the ethical requirements with which the project complies, identifies and assesses the risks involved in the processing of personal data and describes the methodology to address them. In any case, the Consortium, in cooperation with the designated Data Protection Officer (DPO), must monitor and update this Study, as well as ensure the implementation of the measures provided for therein.

In particular, the following were taken into account:

1. Decisions of the Data Protection Authority

2. The Guidelines for the Data Protection Impact Assessment of the Article 29 Working Party (as revised and adopted on the 4th of April 2017)

3. Relevant guidance from the French Commission Nationale de l'Informatique et des Libertés (CNIL)4

4. Relevant guidance from the UK Information Commissioner's Office5

5. Proposed methods of the European Organisation for Cybersecurity (ENISA)

6. Proposal for a Regulation laying down harmonised rules for Artificial Intelligence (European Commission - April 2021)

7. The Treaty on European Union and the Treaty on the Functioning of the European Union (2016/C 202/01)

8. The Charter of Fundamental Rights of the European Union (2012/C 326/02)

9. The European Commission's Ethical Guidelines on the use of AI and data in teaching and learning for Educators (October 2022).

2.2. THE METHOD FOLLOWED FOR THE IDENTIFICATION AND ANALYSIS OF RISKS

The main objective of this study is to identify and document the risks to the rights and freedoms of natural persons arising from the processing of personal data during training using XR technology. Indicatively, such risks include the following:

α) Leakage of personal data,

b) Unauthorised modification of personal data,

c) Loss or theft of personal data.

Scenarios that may lead to the emergence of the identified risks related to the security of the information and the means used to process it are investigated.

For the creation of each scenario, the following elements are evaluated:

1) existing supporting resources,

2) the potential vulnerabilities (mainly in terms of increased risk of malfunction) of supporting resources,

3) any impending risks that may occur as a result of the vulnerabilities,

4) the existing risk control measures,

5) the magnitude of the impact of the risk,

6) the likelihood of the risk occurring.

In particular, for each risk, its severity is calculated, which, in principle, depends on the nature of its possible consequences for natural persons - data subjects, within the meaning of Article 4 paragraph 1 GDPR (in this case, learners and educators). In order to assess the seriousness of a risk, the impact on privacy that occurs as a result of a feared event affecting personal data is considered. Therefore, the two - causally linked - components of the severity of a risk are:

α) The impact of a feared event on personal data,

b) The impact on privacy.

3. IMPLEMENTATION OF A DATA PROTECTION IMPACT ASSESSMENT STUDY ON THE XR4ED PLATFORM

3.1. ASSESSMENT OF THE MEASURES GUARANTEEING THE PROPORTIONALITY AND NECESSITY OF THE PROCESSING IN XR4ED

The Controller has made the following choices in order to comply with the proportionality and necessity requirements of the GDPR:

In particular, as regards the **purposes of the processing:**

They are clearly defined, explicitly described in the legislation and are legal.

The provision of education using XR technology, and, by extension, the development and use of online experiences is in the public interest. More specifically, by introducing the possibility of remote education through XR technology, on the one hand, the constitutional imperative of promoting teaching is served, as is the objective of accessibility and inclusive education in general. On the other hand, it ensures that trainees who are unable to follow the educational process in person, and in particular people with mobility problems or suffering from any form of physical or cognitive disability, will not be alienated from the learning process and the benefit of knowledge.

There is no recording or storage of the experience transmission.

For completeness purposes, it is noted that the collection and use of personal data when using the XR4ED platform especially the traffic data and animation files will follow the principle of data minimisation - after anonymisation - to draw conclusions about education through XR technologies (research purposes). This procedure does not include any ID processing operations, with the exception of the initial application of the anonymisation method nor approved code of conduct. The special categories of personal data generated during the use of the XR4ED platform will not be collected.

A. Legal basis: the legal basis for processing: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller (Art.6§1 f.

e GDPR) and in this context: processing is necessary for compliance with a legal obligation of the Controller (Art.6§1 f. c GDPR).

B. Data minimisation. The indicated recipients are necessary to have access to the data for the implementation of the training programmes in accordance with the provisions of the legislation.

C. Data retention period: personal data is deleted upon completion of the training provision through the XR4ED platform.

3.2. OVERVIEW OF THE MAIN PARAMETERS OF THE TREATMENT

PROCESSING ACTIVITY: Synchronous teaching using XR experiences.

PURPOSE: To provide inclusive learning training using XR technology

DATA CONTROLLER: CELLOCK

Public interest served:

- The continuity of education provision
- Students who are unable to follow the educational process in person should not be alienated from the educational process.
- Accessibility

PROCESSOR: Theoharis Zacharatos, CELLOCK

DATA PROTECTION OFFICERS:

- Anthoulla Fotsiou Psoma (CYENS)
- Neophytos Vlotomas (CELLOCK)
- Kurt Sprengel (Nurogames)

Relevant certifications: N/A

3.3. PERSONAL DATA - RECIPIENTS

PARTICULAR PROCEDURES	PERSONAL DATA - CATEGORIES OF SUBJECTS	SOURCES
1. Creation of an online experience	A) **Educators**: i) Name, ii) Speciality, iii) Email address, iv) Credentials platform user credentials (username, password) to implement the authentication process. B. **Trainees** (i) Name, (ii) Email address, (iii) Any special requirements such as interpreting for disabled persons, (iv) Fingerprints for identification purposes, (v) Skin temperature, (vi) Eye movement data, (vii) Involuntary information such as medical conditions	Platform XR4ED XRED Marketplace
2. Notification of the start of an online experience via a link	(i) full name of the user, (ii) email address	Platform XR4ED XRED Marketplace The data are processed by the relevant educational institution
3. Student Registration in cases where the link to follow the training programme is posted on the platform	i) Full name, ii) educational programme to be attended, iii) username on the platform, iv) email address (It is noted that all	Platform XR4ED XRED Marketplace

	users, by registering, must consent to the sending of informative emails about the online courses they wish to attend and the communication with the respective institution), v) potentially (optionally) the inclusion of additional information about gender, age, level of education etc. that a user wishes to include in his/her profile.	The data shall be submitted to be processed by the person's educational
4. Admission to the transmitted experience	Full name or username chosen by the student for the purpose of attending the course	Platform XR4ED XRED Marketplace The data in question are processed when users enter the XR4ED platform because they are elements of the educational programme
5. Image Activation	A. Educators and Students /Trainees (i) Audio data; (ii) data that may be transmitted incidentally due to the location of the device through which the Subjects participate in the tele-education, if located in a private area; (iii)	Platform XR4ED XRED Marketplace Closed number of users participating in each training programme

	biometric data; (iv) orientation data; (v) environmental data B) Third Persons: (i) Audio data of third persons who are in the same (personal) space as the participants in the training programme. In any case, it is stressed that these categories of data are transmitted in an incidental manner. While it is specified that all the above data can only be transmitted in real-time.	
6. Sound activation	Educators & Students: (i) Audio Data; (ii) Data that may be transmitted incidentally due to the location of the device through which the Subjects participate in the experience if located in a personal space; (iii) Health-related data related to a user's current health, in order to adapt the text and web space accordingly.	Platform XR4ED XRED Marketplace Closed number of users participating in each training programme
7. Further use of the platform	Data that will be stored after being anonymised for research/statistical purposes. In	Consortium

	particular: i) Traffic data, ii) Animated screen files, iii) Operating System Type and Version, v) Platform Version, vi) Actions (logging in/out of the platform, participation in a videoconference, leaving a videoconference) (vii) Training programme information (title, date and time, average and actual duration, connectivity, (viii) Number of videoconferences (ix) Screen sharing/non-sharing sessions, (x) Number of participants (xi) Screen resolution (xiii) Method of accessing the videoconference (via application or navigation software), (xiii) Problem management from other diagnostic information about the platform.	

Table 1: Personal Data - Recipients

3.4. THE RIGHTS OF DATA SUBJECTS

The following table describes the legal and ethical requirements regarding the rights of the Data Subjects and, by extension, how the Controller complies with them:

LEGAL REQUIREMENT	IMPLEMENTATION MEASURE
Right to Information and Transparency - Information on Data Subjects (fair and transparent processing, Art 12, 13, 14 GDPR)	1. Websites with information on how the platform works (Detailed information and instructions for users) 2. Acceptance of the terms of use of the platform and consent forms as a condition of access to the XR4ED online platform.
Obtaining consent (Articles 7, 8 of the GDPR)	The processing is not based on consent, as it serves a public interest and thus a legal obligation established to their satisfaction.
Right of access and portability (Art.15, 20 GDPR)	Users have the right to access their personal data upon request to the Data Protection Officer that is processed during their participation in a training program of the XE4ED online training platform, with the exception of the data that are registered - resulting from the use of the platform if they are not linked to the platform with their real data so that they can be identified. It should be noted that the right to portability cannot be admissibly exercised in the present case because the GDPR does not establish a general right to data portability for cases where the processing of personal data is not based on consent or a contract.

Right to rectification and erasure (Articles 16, 17 GDPR)	These rights may be exercised under the conditions set out in the GDPR and require a request to the Data Protection Officer.
Right to restriction of processing and right to object (Articles 18, 21 GDPR)	A procedure is provided upon request to the Data Protection Officer to allow Data Subjects to object to processing on the basis of their particular situation and to request the restriction of processing, in accordance with the requirements of the GDPR.
Processors (Art. 28 GDPR)	The Processors have provided guarantees that they take all necessary technical and organisational measures to protect the data of the Data Subjects. In particular with regard to privacy and data collection: α) the 'privacy by design' approach (b) Security measures (c) Data protection team

Table 2: Rights of the Data Subjects

In view of the above, no additional protective measures are required

3.5. PROPORTIONALITY STUDY

Training through the XR4ED online platform using XR technology raises the issue of balancing conflicting fundamental rights. The rights under consideration are therefore listed:

A. The right to education and the development of new technologies

The right to education is a fundamental human right enshrined in Article 26 of the Universal Declaration of Human Rights. In particular, quality education aims to ensure the development of a well-rounded human being and is one of the most important tools for the removal of socially excluded children and adults. The rapid evolution of technology offers in Education online platforms that can support the teaching and learning process, which is carried out remotely, while at the same time providing the possibility to design and develop collaborative, interactive and critical-reflective educational activities, which can be carried out remotely, enhancing interaction, active learning, and student autonomy.

B. The protection of personal data

The right to protection from the collection and processing of personal data, according to recital 4 of the GDPR, is not an absolute right but must be assessed in relation to its function in society and weighed against other fundamental rights, in accordance with the principle of proportionality. Moreover, Articles 1§3 and 85 of the GDPR lay down specific rules when weighing the free flow of personal data against the freedom of expression and information respectively.

Therefore, in case of a conflict between the right to personal data and other legal goods and rights, such as the right to education, it is necessary to balance and harmonise them, based on the constitutional principle of proportionality. This is dictated by the need to remove potential conflicts of fundamental rights by balancing interests in each specific case.

In any case, the protection of personal data does not lead to an absolute prohibition of their collection, processing and use, but obliges the common legislator to establish a restrictive institutional framework within which the collection, processing and use of personal data becomes lawful.

More specifically, in relation to education via an online platform, in particular, using modern XR technologies, the proportionality principle examines whether the measure of such education is

appropriate for the provision of the education good. In this respect, it is considered that the measure in question is appropriate and effective, given the familiarity of the pupils with the technology and the accessibility of the disabled.

In any case, the possibilities, and challenges of integrating XR technology in the field of education need to be explored in a harmonious balance with the privacy rights of students and Educators respectively. More specifically, the adoption of Augmented Reality (AR), Virtual Reality (VR) and Mixed Reality (MR) applications and devices, known as Extended Reality (XR), in the field of education offers the possibility of a seamless interaction between machines in a three-dimensional and multidimensional cyberspace.

A basic objection against the system of education through an online platform could be considered that the most important asset and driving force of education is the qualitative interactive pedagogical relationship, which is achieved in face-to-face education. However, the provision of education through XR technologies can be considered equally effective and a key tool in the realisation of the right to education and thus the conflicting constitutional goods are brought in harmony, resulting in the good of education being offered in a manner consistent with the protection of personal data and basic ethical principles. It is also noted that in this way the good of education is also provided without hindrance to persons who, for whatever reason, are unable to attend the experience in person and thus remain in contact with the educational process.

3.6. STUDY OF POTENTIAL CHALLENGES IN RELATION TO THE RIGHTS OF STUDENTS AND EDUCATORS

In order to safeguard the rights and freedoms of the users of the platform, the risks and threats posed by the processing activity are examined and appropriate measures **to** limit/eliminate them are identified.

3.6.1. CHALLENGES-RISKS IN RELATION TO RIGHTS AND TECHNICAL ISSUES

The free development of personality

The question arises as to whether the training provided through the use of the new XR technologies prevents the free development of the users' personalities as they may feel that they cannot express

themselves freely because this method digitises physical processes, collects data from users and environments through sensors and enables computers to guide users through experiences of a purely digital world.

This legitimate fear is countered by the fact that the XR4ED platform already by design follows standard collaborative learning practices by implementing a set of flexible XR services and modern XR tools and the user will retain the right to interrupt the transmission if they deem it necessary, while the learning experiences are combined with sophisticated experiences and tools (games, online quizzes, etc.).

Privacy risks

The possibility of processing a huge amount of information through modern technologies poses a great risk to the privacy of the data subject. In particular, the possibility of constructing an artificial profile of the personality of each individual through the collection, processing and selection of data from various sources, which may not even correspond to the actual personality of the subject, represents a new threat in the field of privacy protection from the collection of information concerning privacy.

The specific risk is considered remote based on the design of the XR4ED platform as the privacy principles are applied, while appropriate measures have been foreseen already by its design in order to: a) provide adequate security b) minimize the possibility of disclosure and collection of personal data, c) properly inform the data subjects about the data protection policy on the platform and c) provide alternatives to the data subject regarding the disclosure and use of the data.

Preserving academic freedom

Furthermore, the risk of restricting the academic freedom of Educators is mentioned. Pupils will attend the lesson from their own personal space (most likely from home) and their family members may attend along with them and interfere with the Educator's work. This risk is mitigated by the adoption of rules of decency in the conduct of the online course, which are communicated to the individual user as part of the educational process. It is also stressed that only users will have access to the course.

Avoiding the collection of third-party data and unintended information

Then there is the potential risk of collecting data from third parties who are in the same room as the users and unintended information such as non-verbal reactions or background data that may provide information about an individual. This issue is effectively addressed by providing instructions (in particular from the person in charge of the training programme during web-based courses) on how to place the electronic device with which users participate in the e-learning in an appropriate location and how to participate in the course from specific areas that are not used by other people while the e-learning is being delivered.

Avoiding leakage of special categories of data

In addition, there is a potential risk that special categories of users' personal data may be disclosed in the context of learning instruction. With regard to this issue on the XR4ED platform, apart from the fact that, as already indicated, the principle of data minimisation will be followed, no special categories of personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information on the subject's sexual life will be collected.

Avoiding marginalisation

The potential risks could include the risk of marginalization of students who cannot participate in the educational process with physical presence but choose the method of education through the XR4ED platform. First of all, it should be stressed that under no circumstances is information relating to the health of the user and the reason for choosing this method of education disclosed. Moreover, it is clear that this method of training is more effective in making difficult theories and complex mechanisms acceptable and comprehensible to students, while at the same time being available in various forms to enable users with disabilities to participate, who are not deprived of the right to education.

Technical failures

The risk of technical failures that could cause the loss of one or more of the platform's security features, such as failures of servers, hard disks, network lines, software failures, etc. is not negligible. With regard to this issue, it is noted that XR4ED has already taken all the necessary security measures to mitigate the

risks and is going to carry out tests and audits at regular intervals to verify the proper functioning of the software.

3.7. TECHNICAL CHALLENGES IN RELATION TO THE DEVELOPMENT OF XR TECHNOLOGIES

Extended development process

In this regard, concerns are raised about the complexity of XR technologies which could potentially limit access for students. In particular, XR systems consist of hardware and software components that need to be carefully coordinated in order to work together, which requires detailed programming and a deep understanding of both hardware and software engineering. In addition, XR applications must be designed with the user experience in mind, requiring developers to consider factors such as user navigation, usability, and aesthetics.

In addition, another challenge is the limited availability of resources as XR technologies are relatively recently available and therefore it can be difficult to find developers with the necessary skills and experience, while the cost of development tools can also be prohibitive. However, considering that the XR4ED platform is provided with the appropriate tools and resources, developers can develop such technologies and this risk should be considered limited.

3.8. STUDY OF SAFETY MEASURES

3.8.1. EXISTING SECURITY MEASURES

The Data Controller has already taken the following security measures to protect personal data:

1. The user has the possibility to stop the transmission at their discretion,
2. The collection and use of personal data for research shall be based on the principle of data minimisation,
3. A Data Protection Officer will be appointed,
4. A Data Management Plan is to be developed which will define how personal data will be collected,
5. The purpose of the collection and processing of personal data will be clear and defined,

6. The biometric, environmental and orientation data that will be extracted will be protected by the DevOps environment which will allow access only to the absolutely necessary data that is essential for the proper functioning of the software,
7. The access of a certain user to the platform will be authorised by the person in charge,
8. Access control to data has been activated so that only authorised persons can access the data for a specific purpose,
9. A limitation of the search results to a certain number has been activated so that no bulk data can be extracted,
10. The servers are protected within a private network, behind firewalls,
11. There is physical protection of the servers in the platform's data centre in an area with controlled access. There is also a backup remote point of retention of user data for protection in the event of a disaster,
12. The transmitted images can only be viewed by certified users of the specific training program without the right to record the image with their own means, as recording through the platform is not allowed,
13. From an organisational point of view, there is a data mapping and information management system (Findable, Accessible, Interoperable and Reusable (FAIR) outputs),
14. There are Data Recovery procedures,
15. Policies and Procedures are in place to manage breaches and other security incidents,
16. There are Data Protection Policies and Procedures in place (Retention Period, Secure Deletion of IDs, Satisfaction of Data Subjects' Rights),
17. An Incident and Breach Management Plan is in place,
18. Data anonymisation plan.

The description of the above measures will be reviewed and updated on a regular basis, at which time any amendments/improvements will be proposed.

3.9. EXISTING MEASURES TO MEET ETHICAL REQUIREMENTS

The XR4ED platform has already adopted the following measures to comply with the ethical requirements. In particular:

1. The platform provides accessibility to all learners, thus avoiding any discrimination based on ethnicity, race, gender, sexual orientation, social origin, language, religion, physical ability, age, educational level, and socio-economic circumstances,
2. Studies are conducted with full respect for human rights, dignity, and safety of persons,
3. Promotes understanding and respect for gender equality,
4. All individuals are offered the opportunity to participate actively in a free society,
5. Full transparency is provided on the methods and operating characteristics,
6. Content warning labels are included which the user can filter out to avoid the specific content they do not want,
7. Respect user privacy in cases where multiple users share the same virtual space collaboratively.

3.9.1. IDENTIFICATION AND ASSESSMENT OF RISKS RELATED TO THE PROTECTION OF PERSONAL DATA

The following tables describe the following information for each risk: 1. The sources of Risk 2. The Main Defects. 3. Possible Effects 4. Estimated Risk Severity 5. The estimated probability of occurrence of the hazard.

3.9.2. RISK OF UNLAWFUL ACCESS TO PERSONAL DATA COLLECTED BY THE PLATFORM

SOURCES OF RISK	MAIN DEFECTS	POSSIBLE EFFECTS	ESTIMATED RISK SEVERITY	ESTIMATED PROBABILITY OF OCCURRENCE OF THE RISK
The data collected will be kept in the infrastructure of the processor: therefore the main sources of risk are: 1) Unauthorised personnel 2) Malicious "intruders" (hackers/crackers)	1) Interception of Authorized User Data 2) Interference with the computing infrastructure of the controller and the processor 3) Granting (by mistake) access rights to unnecessary information	1) Disclosure of data: name, email address and metadata (from which the number and type of online courses taken and their duration can be deduced). 2) Unauthorised use of data (examples include the use of the user's e-mail address in services which do not implement an identification or verification procedure of the e-mail address	**Unit: 2 (TWO)** Justification: The infrastructure of the processor will hold user data, i.e. registration data (name, email address, username, etc.) and metadata resulting from the use of the platform. The impact is considered to be limited according to the classification proposed by the CNIL. (Privacy Impact Assessment, 2018).	**Unit: 1 (ONE)** Justification: The measures in place for the operation of the platform are considered sufficient to counter malicious attacks and prevent unauthorised access to its infrastructure.

		when users register). 3) Receiving unsolicited communication and consequently annoying the Subject 4) Emotional distress of the Subject (such as, for example, anxiety about how his/her personal data will be used) 5) Dissatisfaction of the Subject from the leakage of his/her personal data to the knowledge of an unauthorised third party 6) Reduction of trust in the applied training process through the platform		

		which may also lead to refusal to participate in it.		

Table 3: Risk Of Unlawful Access To Personal Data Collected By The Platform

3.9.3. RISK OF UNLAWFUL ACCESS TO PERSONAL DATA DURING TRANSMISSION

SOURCES OF RISK	MAIN DEFECTS	POSSIBLE EFFECTS	ESTIMATED RISK SEVERITY	ESTIMATED PROBABILITY OF OCCURRENCE OF THE RISK
1) Students 2) Educators 3) Other third parties from the users' environment (such as for example escorts of people with physical disabilities), acting with the intention of accessing the online classroom. 4) Malicious "intruders" (hackers/crackers)	1) Visual contact with the screen of the person participating in the tele-education through the platform - sharing the same virtual space. 2) Intervention in the applications of the platform, where the links to online participation in the training program are posted 3) Access (malicious with intent or passive) to a device where	1) Disclosure of data that may have been obtained - but not recorded during access 2) Subjects' concern if access is perceived - feeling of privacy intrusion without causing irreversible harm 3) Reduction of trust in the applied training process through the platform which may also lead to refusal to participate in it. 4) Monitoring of unwanted content	**Unit: 2 (TWO)** Justification: Illegal-malicious access concerns in particular biometric data - image data (and any environmental data disclosed). The main threats, in addition to malicious attacks on XR4ED software, may occur individually and affect one user at a time. The impact is considered to be limited according to the classification proposed by the	**Unit: 2 (TWO)** According to the measures in place, the likelihood of the risk is limited

	the XR4ED login credentials are stored 4) Access to a student's personal device where the link to the online participation is stored 5) Interception of XR4ED access credentials for the purpose of using the link and entering the online training program. 5) Malicious attack on the infrastructure of the processor for the purpose of intercepting	in case the filtering function does not work.	CNIL. (Privacy Impact Assessment, 2018).	

Table 4: Risk Of Unlawful Access To Personal Data During Transmission

3.9.4. RISK OF CHANGE OF PERSONAL DATA

SOURCES OF RISK	MAIN DEFECTS	POSSIBLE EFFECTS	ESTIMATED RISK SEVERITY	ESTIMATED PROBABILITY OF OCCURRENCE OF THE RISK
1) Unauthorised personnel 2) Appointed Processing Subcontractors 3) Malicious "intruders" (hackers/crackers)	1) Access to and alteration of personal data 2)Violation of personal autonomy	1) Feeling of invasion of privacy (noting that no irreversible damage is caused) 2) Reduction of trust in the applied training process through the platform, which may lead to refusal to participate in it. 3) Keeping data that is not accurate 4) Temporary interruption of the training programme	**Unit: 2 (TWO)** **Justification:** Justification: The interference concerns in particular the data held in the infrastructure of the processor. The impact is considered to be limited according to the classification proposed by the CNIL.	**Unit: 1 (ONE)** According to the measures in place, the likelihood of the risk is negligible.

		5) Malfunctioning of input methods ***<u>In addition</u>***, in the event that the alteration takes place on data held in the infrastructure of the processor, inaccurate data may be obtained and therefore the results/conclusions of surveys and statistical analyses based on altered data (following anonymisation) may be incorrect.		

Table 5: Risk Of Unlawful Access To Personal Data During Transmission

3.9.5. RISK OF LOSS OF PERSONAL DATA

SOURCES OF RISK	MAIN DEFECTS	POSSIBLE EFFECTS	ESTIMATED RISK SEVERITY	ESTIMATED PROBABILITY OF OCCURRENCE OF THE RISK
1) Unauthorised personnel of the processor 2) Appointed sub-processors 3) Malicious 'intruders' (hackers/crackers) 4) Destruction on the premises of the processor 5) Overloading (source of risk of temporary loss risk, which is understood only for data stored kept on the	1) Access to personal data user data and delete them. 2) Temporary inability to provide the service and therefore loss of transmitted data and temporary loss of data that kept in the infrastructure of the processor. 3)Physical destruction of infrastructure (domestic network) of the processor was	1) Temporary suspension of educational programmes. 2) Degradation of the quality of online experiences. 3) Re-creation of educational programs (in case of definitive loss of data) 4) Limitation on the availability of data that kept on the infrastructure of the processor. 5) Reduction of trust in the training process implemented	**Unit: 2 (TWO)** **Justification:** The loss in this case concerns the data held in the infrastructure of the processor. Impacts are considered to be limited according to the classification proposed by the CNIL.	**Unit: 1 (ONE)** **Justification:** The security measures in place are considered sufficient to deal with malicious attacks and to mitigate the risk. It is emphasised that the probability of the risk occurring is considered negligible.

processor's infrastructure (after anonymisation).	kept and/or through the which data are transmitted.	through the platform, which may lead to the refusal to participate in it. Furthermore, it is noted that there will be no possibility to carry out surveys and statistical studies.		

Table 6: Risk Of Loss Of Personal Data

It is evident from the details presented in the above tables (risk mapping) that the risks described are **acceptable** in terms of severity and probability of occurrence.

Further, the **impact on personal data** was captured above using the rating scale ("Likert") as follows:

LEVEL	UNIT	DESCRIPTION
INSIGNIFICANT	1	The event in question does not affect personal data or affects them on a very small scale.
LIMITED	2	The event in question affects personal data on a limited scale.
IMPORTANT	3	The event in question affects personal data on a medium or medium to large scale.
GREAT	4	The event in question affects personal data on a large or very large scale.

Table 7: Likert Scale For Measuring The Impact On Personal Data

In determining the scale, it is noted that the following were taken into account: a) the number of subjects involved, b) the volume and scope of the data, c) the duration and nature of the processing (permanent/temporary) and d) the geographical extent of the processing.

Similarly, the effects on privacy were captured using a Likert scale as follows:

LEVEL	**UNIT**	**DESCRIPTION**
INSIGNIFICANT	1	Natural persons/subjects are slightly affected (data re-importation, irritation, annoyance).
LIMITED	2	Natural persons face significant problems which are not insurmountable (additional costs, denial of access to services, lack of trust, stress).
IMPORTANT	3	Substantial impacts on natural persons which are reversible and can be overcome through serious difficulties.
GREAT	4	Natural persons face significant or irreversible impacts that they cannot overcome.

Table 8: Likert scale for capturing the effects on privacy

4. CONCLUSIONS

Regarding the approach to privacy and ethical issues that will arise from the use of the XR4ED platform, by virtue of this study you conclude that:

1. The fundamental principles of personal data processing are not violated. The processing activity complies with the principle of proportionality and the data are to be collected in accordance with the provisions of the relevant legislation and the conditions laid down by that legislation.
2. There will be transparency and the information required by Articles 12-13 of the GDPR will be provided to Data Subjects.
3. The Data Controller in cooperation with the processor is to satisfy the rights of the Data Subjects.
4. The risks to the rights and freedoms of Data Subjects were assessed and deemed acceptable, always subject to the implementation and compliance with the proposed measures.
5. The necessary efforts will be made to ensure that the personal data held and processed by the platform is always accurate and up to date.
6. Appropriate technical and organisational measures are to be taken so that personal data are processed in a way that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage. In addition, the adequacy and effectiveness of these measures shall be reviewed at regular intervals.
7. Regarding the use of new XR technologies, it is considered that the transparency obligations for human-interacting systems are respected, and natural persons will be properly informed about the operation of the platform (2021).
8. Essential ethical requirements are met, and all activities will be designed with respect for the dignity of the individual.
9. A fair learning experience is ensured.

References

1	*Aims and values* (no date) *European Union*. Available at: https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en (Accessed: 15 September 2023).
2	Angelides, P., Stylianou, T. and Gibbs, P. (2006) 'Preparing Educators for Inclusive Education in cyprus', *Teaching and Educator Education*, 22(4), pp. 513–522. doi:10.1016/j.tate.2005.11.013.
3	Basdekis, I. (2013) 'Ηλεκτρονική Προσβασιμότητα και Αναπήρια (Hellenic)', *National Confederation of Disabled People - Hellas (ESAEA* [Preprint]. doi:10.13140/2.1.3560.6089.
4	Besemer, L. and Newton, S. (2020) *Privacy and data protection based on the GDPR: Understanding the general data protection regulation*. 's-Hertogenbosch: Van Haren Publishing.
5	Booth, T. (2011) *Index for inclusion: Developing learning and participation in schools*. Bristol: Centre for Studies on Inclusive Education.
6	Frąckiewicz, M. (2023) 'Introduction to Extended Reality (XR): An Overview of the Technology', *TS2*, 24 March. Available at: https://ts2.space/en/introduction-to-extended-reality-xr-an-overview-of-the-technology/ (Accessed: 15 September 2023).
7	Kalampouka Giannopoulou, P. (2020) *ΔΙΚΑΙΟ ΣΥΝΑΛΛΑΓΩΝ Ειδικά Θέματα* (1 vols). 2nd edn. Athens: Law Department.
8	Kanellos, L. (2023) *THE GDPR HANDBOOK* (1 vols). 2nd edn. Athens: Law Department.
9	Kennedy, G.E. (2019) *Data Privacy Law: A practical guide to the GDPR*. Middletown, DE: G.E. Kennedy.
10	Loreman, T. (2017) 'Pedagogy for inclusive education', *Oxford Research Encyclopedia of Education* [Preprint]. doi:10.1093/acrefore/9780190264093.013.148.
11	Milkaite, I. and Lievens, E. (2019) 'Child-friendly transparency of data processing in the EU: From legal requirements to platform policies', *Journal of Children and Media*, 14(1), pp. 5–21. doi:10.1080/17482798.2019.1701055.
12	*Privacy Impact Assessment* (2018) *National Commission on Informatics and Liberty*. Available at: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf (Accessed: 15 September 2023).
13	*Process personal data lawfully* (no date) *EDPB*. Available at: https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en (Accessed: 15 September 2023).
14	*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS* (2021) *Eur-lex Europa*. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (Accessed: 15 September 2023).