Co-funded by
the European Union

ADMIT

Taxonomy of the ethical issues related to the use of LLM/ Generative AI systems

EADTU
JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ
UNED
HELLENIC OPEN UNIVERSITY
ANADOLU UNIVERSITY
FernUniversität in Hagen
Open Universiteit
UOC Universitat Oberta de Catalunya
FernUni.ch
UniDistance.ch
UNIVERSITÀ TELEMATICA INTERNAZIONALE UNINETTUNO
The Open University
OPEN UNIVERSITY OF CYPRUS
www.ouc.ac.cy

The research reported in this document was carried out in the ADMIT EU funded project. Proposal ID 101134520 under the call ERASMUS-2023-PCOOP-ENGO

Citation:
Carbonel, H., Triantafyllopoulos, L., Kalles, D., Kameas, A., Jullien, J.M. & Antonaci, A. (2024). Taxonomy of the Ethical Issues Related to the Use of LLM/ Generative AI Systems in Higher Education. (Research Report No. 5.2, ADMIT). Zenodo. DOI: 10.5281/zenodo.17864328

License used: This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License: https://creativecommons.org/licenses/by-sa/4.0/.

ShareAlike: If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Executive Summary

This deliverable presents the Taxonomy for the Ethical Use of Generative AI in Higher Education, developed within the ADMIT project to support the responsible adoption and use of Generative AI across higher education. The taxonomy provides a structured framework that translates key ethical principles and legal requirements into practical dimensions and guiding questions that can inform the planning, implementation, and evaluation of GenAI applications in educational contexts.

The taxonomy covers eight ethical dimensions: 1) Educational Impact and Integrity; 2) Privacy and Data Governance;3) Societal, Individual and Environmental Wellbeing; 4) Teacher and Student Agency and Oversight; 5) Diversity, Non-discrimination and Fairness; 6) Accountability; 7)Transparency, and 8) Technical Robustness and Safety, complemented by a legal dimension based on the General Data Protection Regulation (GDPR), the AI Act, and relevant intellectual property considerations. Together, these dimensions provide a comprehensive framework for identifying ethical challenges, supporting reflective decision-making, and promoting responsible AI practices in higher education.

Table of contents

Introduction

The taxonomy for the ethical use of GenAI in higher education is based on the existing AI frameworks of AI in education (Commonwealth of Australia, 2024; Directorate-General for Education, 2022; Floridi & Cowls, 2019; High-Level Expert Group on AI, 2019; Holmes et al., 2023; Şenocak et al., 2024; UNESCO, 2021) to which we have added the dimension specific to the field of teaching and learning 'Ethical Impact and Integrity' (Bozkurt, 2024; Holmes, 2024; Holmes et al., 2022; Sahlgren, 2023; Selwyn, 2023), as well as a legal section based on the GDPR, AI Act, and emerging IP rights. The questions were taken from the literature, selected through an iterative process with the developers of the taxonomy based on those most relevant to the use of GenAI in a higher education context. The legal aspects were reviewed and enhanced by EPIA members.

The taxonomy will be used by higher education stakeholders (students, teachers, institutional managers, GenAI technology developers) to consider the different ethical dimensions of the planned use of GenAI in higher education. The legal aspects are binding. Otherwise, the decisions are highly context-dependent and will often require weighing opposing considerations and priorities (e.g. the need to learn to use GenAI vs its negative environmental impact; data anonymisation vs. the need to trace individual data to personalise support). The questions should be adapted to the audience and use-case.

The appendices provide supplementary material supporting the taxonomy. They include the legal definitions underpinning the legal section of the taxonomy, as well as a summary of the legal dimensions and their corresponding guiding questions presented in tabular form.

Taxonomy for the ethical use of Generative AI in Higher Education

Table 1 presents the taxonomy for the ethical use of Generative AI in higher education. It is structured around a set of interrelated ethical and legal dimensions, each supported by guiding questions that help users examine the implications of a particular GenAI application or use case. The questions are intended to encourage systematic reflection on issues such as responsibility, fairness, human oversight, transparency, privacy, accessibility, sustainability, and educational integrity. Rather than offering fixed answers, the taxonomy supports informed discussion and context-sensitive decision-making, recognising that different uses of GenAI may involve competing priorities, risks, and potential benefits.

Dimensions	Description	Questions	References
Educational Impact and Integrity	Educational Impact and Integrity focuses on the alignment with pedagogical approaches, supporting learning, adhering to educational values, and upholding academic integrity.	What is the purpose of using GenAI in your teaching or learning? What problems are you trying to solve?	(9, 10, 11)
		Does your use of GenAI support your pedagogical approach?	(9)
		Is there evidence that the GenAI system is supporting learning as intended? Can the technology do what is expected of it?	(9)
		How is the effectiveness and impact of the AI system being evaluated and how does this evaluation consider key values of education? Does the evaluation include the effect on the role of teachers, mental health, social interactions, etc.?	(3, 9, 10)
		Is it a problem that GenAI is not trustworthy? Should students be able to check and evaluate the sources?	(9)
		Is GenAI used in a way that upholds the values of academic integrity such as honesty, trust, fairness, respect, and responsibility? Does the technology respect intellectual property, cite its sources and avoid plagiarism?	(9, 17)
		What role is foreseen for the teacher, the institution, and students when the AI system is used?	(11)
		What do we risk losing through the use of AI systems?	(11)
Privacy and Data Governance	Privacy and Data Governance focus on respect for privacy, quality and integrity of data, and access to data.	Does the suggested use of GenAI comply with the GDPR?	(3, 20)
		Is it possible to customise the privacy and data settings?	(3)
Societal, Individual, and Environmental Wellbeing	Societal, Individual and Environmental Wellbeing focuses on sustainability and environmental friendliness, social and individual impact, societal well-being, and democracy.	GenAI has a strong environmental impact and is expensive, does its use add to the learning experience something that could not be done otherwise?	(9)
		What negative effect may this use of GenAI have on society or the individual? Does the use of the GenAI system create any harm or fear for society or individuals?	(3)
	Teacher and Student Agency and Oversight focuses on	Are teachers and students equipped with the necessary digital and AI literacy skills to make informed decisions?	(9, 10)

Teacher and Student Agency and Oversight	digital and AI literacy, informed decision-making, autonomy in technology use, and mechanisms for monitoring and support.	Is the teacher free to decide whether to use the GenAI technology or not in their module? Is there a mechanism for learners to opt-out without being at a disadvantage?	(3, 9)
		Is the GenAI technology manipulating or misleading students?	(9)
		Are procedures in place for teachers to monitor and intervene, for example in situations where empathy is required when dealing with learners?	(3)
		Does the GenAI system empower learners and teachers?	
Diversity, Non-discrimination, and Fairness	Diversity, Non-Discrimination, and Fairness focuses on accessibility, universal design, the avoidance of unfair bias, and stakeholder participation, allowing use regardless of age, gender, abilities, or characteristics, with a particular focus on students with special needs.	Is the technology accessible to everyone in the same way, without barriers? E.g, governmental regulations, limited internet access, insufficient infrastructure, disabilities or special education needs.	(3)
		What biases are present in the training data? Including cultural biases, marginalised groups, language, etc.	(9, 10)
		Are we diminishing quality education for certain groups, are AIED systems biased against some groups, and are some other groups being ignored? What impact could the biases have on the learners?	(9, 10)
		Are procedures in place to detect and deal with biases or perceived inequalities that may arise?	(3)
Accountability	Accountability focuses on auditability, minimization and reporting of negative impact, trade-offs, and redress.	(Institutional level) Is there a Service Level Agreement in place, clearly outlining the support and maintenance services, responsibilities, and steps to be taken to address reported problems?	(3)
		Who is responsible if something goes wrong?	(9, 10)
		Is there an easy route for complaints or redress?	(11)
Transparency	Transparency focuses on traceability, explainability, and communication.	Is the dataset used for training known? Is the system's model visible and inspectable in a way that can be understood by teachers and students?	(8, 10)
		Was the AI system designed and implemented in such a way that it offers clear and certain justifications for every action it takes?	
		If there is no or limited transparency in how the technology works, what implications does this have for teaching and learning?	(8, 10)
Technical Robustness and Safety	Technical Robustness and Safety focuses on security measures, system monitoring, regular checks, and	Is there sufficient security in place to protect against and monitor data breaches and data poisoning? Is there a contingency plan in case of accident?	(3)
		Are there regular checks to ensure the correct functioning of the system?	(3)
		What happens if the technology is no longer available?	(9, 10)

	contingency planning to ensure correct functioning and reliability.		

Appendices

Appendix A. Legal Definitions

This appendix provides the legal definitions referenced in the legal section of the taxonomy. The definitions are based on the GDPR, the AI Act, and relevant intellectual property legislation.

Table A1. Legal definitions used in the taxonomy

Term	Definition	References
Accountability	The obligation of an entity to be responsible for its actions, and to demonstrate and ensure compliance with applicable standards and regulations	In GDPR
Accuracy	Entails maintaining the correctness of data and updating it as necessary. Every reasonable measure must be taken to promptly erase or correct any personal data that is found to be inaccurate, considering the purposes for which it is processed.	In GDPR
Controller	A natural or legal person, public authority, agency, or other body that determines the purposes and means of processing personal data, either on their own or jointly with others.	In GDPR
Data Subject	An identifiable natural person 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.	In GDPR

General Purpose AI Model	An AI system that, often trained with extensive data through self-supervision, demonstrates broad versatility and competence across a diverse array of tasks. This adaptability allows it to be integrated into various downstream systems or applications, irrespective of how the model is marketed. This definition excludes AI models designated solely for research, development, or prototyping prior to market release.	In AI ACT
Integrity and confidentiality	The processing of personal data in a way that ensures its security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage. This is achieved through the application of suitable technical and organizational measures.	In GDPR
Joint-controller	Two or more entities, such as controllers, that collaboratively determine the purposes and means of processing personal data, such as websites utilizing third-party cookies. Recommendations for joint controllership include establishing a transparent arrangement that is also accessible to the data subjects	In GDPR
Personal Data	Any information relating to an identified or identifiable natural person ('data subject')	In GDPR
Data Minimisation	The principle that a data controller should restrict the collection of personal information to only what is directly relevant and necessary to achieve a specific purpose.	In GDPR
Deployer	A 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.	In AI ACT
Fairness	The principle that data should be processed in a manner that is just, equitable, and free from bias, ensuring that it does not harm or mislead individuals. This is crucial in the deployment and regulation of AI systems.	In GDPR
Market surveillance authority	The national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020 (Ref. Fundamental Human Rights Assessments (FRIA);	In AI ACT
Notifying authority	The national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring (Ref. Conformity assessments, FRIA).	In AI ACT

Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	In GDPR
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller	In GDPR
Provider	A natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge	In AI ACT
Purpose Limitation	The principle that data should be collected and processed solely for the specific purposes initially stated. Exceptions include use for archiving in the public interest, scientific or historical research, or statistical purposes, provided they are deemed compatible with the original intent as assessed under Article 6.4 of the GDPR.	In GDPR
Right not to be subjected of Automated Decision Making	The right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects or similarly significantly affects a data subject.	In GDPR
Right of Access	This right ensures that individuals have the ability to confirm whether their personal data is being processed, access the data itself, and receive comprehensive information about the processing activities. Data subjects can request copies of their personal data, inspect files, or obtain oral information, transcripts of relevant documents, and print-outs or summaries of the data in an intelligible form. These provisions may be made available through various methods such as email, physical mail, or self-service tools. The right of access promotes transparency by allowing individuals to understand and verify the extent, nature, and purpose of data processing conducted by the controller.	In GDPR
Right to be forgotten	The right to request de-listing	In GDPR

Right to Erasure	The right to have one's data deleted without undue delay. Exception: For archiving purposes in the public interest, scientific or historical research or statistical purposes in accordance with Art 89 (1) if erasure is likely to render impossible or seriously impair the objectives of that processing	In GDPR
Right to Object	The right that grants individuals the ability to oppose the processing of their personal data, based on considerations specific to their personal situation. Processing must be halted by the controller unless compelling legitimate reasons for the processing are proven, which outweigh the individual's interests, rights, and freedoms, or if the processing is essential for legal claims.	In GDPR
Right to Portability	The right to receive personal data which the data subject has provided to the controller in a structured, commonly used, machine-readable format. Under these conditions: processing based on consent or necessary for the performance of a contract and processing by automated means.	In GDPR
Right to Rectification	The right to obtain without undue delay the rectification of inaccurate data or to have incomplete data completed.	In GDPR
Storage limitation	The principle that personal data should not be retained for longer than necessary. Data must be erased or anonymized once it is no longer required for its intended purpose. Organizations are advised to establish specific retention periods for each category of personal data collected. However, data may be stored for extended periods if processed solely for archiving in the public interest, scientific, historical research, or statistical purposes as per Article 89(1) of the GDPR, provided that adequate technical and organizational measures are in place to protect the rights and freedoms of the data subject.	In GDPR
Transparency	The requirement to process data in transparent manner	In GDPR

Appendix B. Legal Dimensions and Guiding Questions

This appendix summarises the legal dimensions included in the taxonomy together with the corresponding guiding questions to support their interpretation and application.

Disclaimer: users should check with legal experts depending on their specific applications of AI. The taxonomy was developed with legal experts and in reference to legal sources, however it is subject to change.

Table B1. Legal dimensions and guiding questions

EU regulations	Description	Questions	References
General Data Protection Regulation (GDPR)	**Scope of the GDPR:** The GDPR applies to the processing of **personal data*** by both automated and manual methods, as long as the data is part of, or intended to be part of, an organized filing system. It also applies to the processing of personal data carried out by a controller or processor within the scope of their business activities.	Does the AI system process personal data*?	**(GDPR, art. 2 and 3)**
		What personal data will you be collecting?	**(GDPR, art. 4(1), 13, 14 and 30(1)(c))**
	Special Categories of Personal Data: The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited. A list of exceptions apply. Two of the main ones are if the data subject has given consent or if there are reasons of public interest.	Does your organisation process data concerning protected characteristics? If so, have the subjects given explicit consent?	**(GDPR, art. 9)**
		Are the activities that require personal data* processing considered legitimate?	**(GDPR, art. 5(1)(a), 6 and, where applicable, 9)**
	Processing	Have you defined the processing activities of personal data through the AI Systems?	**(GDPR, art. 4(2), 24 and 30)**

	Lawfulness: Legal Basis to process personal data. The legal bases that allow the processing of personal data are the following: Consent, contract, legal obligation, vital interest, performance of a task carried out in the public interest. The consent needs to be "freely given, specific, informed and an unambiguous indication of the data subjects' wishes". In case of public interest processing personal data for research purposes can be considered an exception: Fairness*; Transparency*; Purpose limitation*; Storage limitation*; Data minimisation*; Data accuracy*; Integrity and confidentiality*; Accountability: The controller shall be responsible for and be able to demonstrate compliance.	Have you put measures in place to ensure that the personal data are processed in a secure and lawful manner?	**(GDPR, art. 5, 6, 24 and 32)**
		Does your organisation take into account, any potential risks such as accidental loss, destruction or damage?	**(GDPR, art. 5(1)(f), 24 and 32)**
		Do you have a process in place for students to give an informed, free and specific consent to the processing of their personal data by an AI system?	**(GDPR, art. 4(11), 6(1)(a), 7 and, where applicable, 8)**
		Have you set up retention periods and procedures in the organisation to delete or anonymize personal data?	**(GDPR, art. 5(1)(e), 13(2)(a), 14(2)(a) and 17)**
		Does the use of AI pursue a purpose of public interest, or engage in scientific or historical research?	**(GDPR, art. 6(1)(e), 9(2)(j) and 89)**
		Is the personal data accurate? Are there pathways to ensure inaccurate personal data can be erased or updated?	**(GDPR, art. 5(1)(d), 16 and 17)**
		Have you considered reducing the amount of personal data so that only adequate, relevant and limited personal data - necessary for the purpose identified- are processed through AI System?	**(GDPR, art. 5(1)(c) and 25)**

		Have you put in place a Privacy Policy or Notice specifically for the processing of personal data through AI Systems?	**(GDPR, art. 5(1)(a) and 12-14)**
		Is the personal data collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes?	**(GDPR, art. 5(1)(b) and 6(4))**
	Data Subject* Rights		
	Right of Access*; Right to Rectification*; Right to Erasure*; Right to be forgotten*; Right to Object*; Right to Portability*; Under these conditions: processing based on consent or necessary for the performance of a contract and processing by automated means; Right not to be subjected of Automated Decision Making	Have you put in a place an access point to personal data so that the data subjects are aware that you are collecting their personal data?	**(GDPR, art. 12-23; in particular art. 13-15)**
		Legal justification for the data processing activity: Has the data subject given consent to the processing of his or her personal data for one or more specific purposes?	**(GDPR, art. 6(1)(a) and 7)**
		Is personal data encrypted, pseudonymized, or anonymized wherever possible?	**(GDPR, art. 25 and 32(1)(a); see also art. 4(5))**
		Has clear information been provided about the data processing and legal justification to the data subject?	**(GDPR, art. 5(1)(a) and 12-14)**
General Data Protection Regulation (GDPR)		Do you have a process in place for students and teachers to easily request and receive all the personal data that has been collected/processed about them?	**(GDPR, art. 12 and 15)**

		Do you have a process in place for students and teachers to easily correct or update inaccurate or incomplete information?	**(GDPR, art. 12 and 16)**
		Do you have a process in place for students and teachers to easily request to have their personal data deleted?	**(GDPR, art. 12 and 17)**
		Do you have a process in place for students and teachers to easily ask you to stop processing their data?	**(GDPR, art. 12, 18 and 21)**
		Is it easy for students and teachers to receive a copy of their personal data in a format that can be easily transferred to another company?	**(GDPR, art. 12 and 20)**
		Does the organisation have a procedure to give updated information to the data subject in case that he or she objects?	**(GDPR, art. 12, 19 and 21)**
		Does the organisation intend to implement an Automated Decision-Making process through the use of AI systems?	**(GDPR, art. 22; see also art. 13(2)(f), 14(2)(g) and 15(1)(h))**
	Prohibition of Automated Decision Making. Exceptions.	Do you have a procedure to protect student and teachers' rights when you make decisions about them based on automated processes?	**(GDPR, art. 22(3); see also art. 13(2)(f), 14(2)(g) and 15(1)(h))**
	Processor*	Does the organisation or institution process data for research purposes serving other organisations' interests?	**(GDPR, art. 4(8), 28 and 29; art. 89 where applicable)**

		Does the organisation collect, processes, store or transmit personal data on behalf of other entities or groups of entities?	**(GDPR, art. 4(8), 28 and 29)**
General Data Protection Regulation (GDPR)	**Data Transfers:** Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. **This transfer takes place when an organisation makes personal data available to a person which is outside of the legal jurisdiction of one of the countries of the EU.**	Is your institution collaborating with international partners or hosting data outside the EU?	**(GDPR, art. 44-49)**
		Is your institution going to use third-party vendors or cloud services to process data?	**(GDPR, art. 28 and 32; art. 44-49 where an international transfer is involved)**
		Is your institution going to use a third-party-AI System provider that will process personal data?	**(GDPR, art. 28 and 32; art. 44-49 where an international transfer is involved)**
	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes: Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and	Has your organisation technical and organisational measures to minimise the use of personal data (data minimisation)?	**(GDPR, art. 5(1)(c), 25 and 89)**

	safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. Where personal data are processed for achieving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.		
	Controller*	Who initiates and who decides on the processing of personal data?	**(GDPR, art. 4(7))**
		Why is data being processed? What is the purpose and the means of the organisation to process personal data?	**(GDPR, art. 4(7), 5(1)(b) and 6)**
		Is the organisation processing personal data with third parties?	**(GDPR, art. 26 and/or 28, depending on the parties' roles)**
		If yes, do they serve the same or different purpose in processing the data?	**(GDPR, art. 4(7)-(8), 26 and 28)**
		If yes, have you established their role in data processing?	**(GDPR, art. 26, 28 and 29)**

	Data Protection Officer role: an organisation needs a Data Protection Officer if they are public bodies or if the core activities of the controller or processor require regular and systematic monitoring of data subjects on a large scale. **The Data Protection Officer needs to inform and advise the controller and if it applies, the processor, and monitor compliance with GDPR and internal rules and regulations and provide advice on Data Protection Impact Assessments (DPIA).**	Who is responsible for ensuring GDPR compliance, or compliance with local (national) regulations, across the institution?	**(GDPR, art. 24 and 37-39)**
		Does the institution have a Data Protection Officer?	**(GDPR, art. 37)**
		Are there internal data protection guidelines within the institution?	**(GDPR, art. 24(1)-(2), 25 and 32)**
		Apart from the DPO, is your staff sufficiently trained and aware of data protection?	**(GDPR, art. 32(4) and 39(1)(b))**
		Is your AI system subjected to a DPIA?	**(GDPR, art. 35)**
		Do you have a process in place to notify the authorities and your data subjects in the event of a data breach?	**(GDPR, art. 33 and 34)**
		Is there an independent and administrative support in your organisation to promote awareness about the compliance with data protection obligations and principles?	**(GDPR, art. 37-39; see also art. 24)**

Artificial Intelligence Act (AI Act)	**Provider***	Are you considered a **Provider*** based on the definition provided by the Regulation?	(AI Act, art. 1)
		Are you considered a public authority*?	(AI Act, art. 1)
		Are you familiar with your legal and ethical obligations as a **Provider*** of an AI system?	(AI Act, art. 1)
	Deployer*	Are you considered a **Deployer*** based on the definition provided by the Regulation?	(AI Act, art. 1)

		Are you familiar with your legal and ethical obligations as a **Deployer*** of an AI system?	(AI Act, art. 1)
	Notifying authority*	Is it clear when you should contact your notifying authority* and with what information?	(AI Act, art. 1)
	Market surveillance authority*	Is it clear when you should contact your market surveillance authority* and with what information?	(AI Act, art. 1)
	Risk classification: Unacceptable, high, medium or low risk AI systems		
	Unacceptable AI systems: - Deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm. - Exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm. - Biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data. - Social scoring, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people. - Assessing the risk of an individual committing criminal offences solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity. - Compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage. - Inferring emotions in workplaces or educational institutions, except for medical or safety reasons. - 'Real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except	Is your AI system considered unacceptable?	(AI Act, art. 5)

	when: - searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited; - preventing substantial and imminent threat to life or foreseeable terrorist attack; or - identifying suspects in serious crimes (e.g., murder, rape, armed robbery, narcotics and illegal weapons trafficking, organised crime, environmental crime, etc.).		
	High-risk AI Systems in education and vocational training: (a) AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels; (b) AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels; (c) AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels; (d) AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.	Is your AI system considered high-risk?	(AI Act, art. 6.2) Annex III: High-risk AI systems
	Limited Risk AI Systems: Limited risk refers to the risks associated with a lack of transparency in AI usage. The AI Act introduces specific transparency obligations to ensure that humans are informed when necessary, fostering trust. For instance, when using AI systems such as chatbots, humans should be made aware that they are	Does the AI tool used substantially influence decision making?	(AI Act, Recital 53)
		Does the task performed by the AI system intend to improve the result of a previously completed human activity?	(AI Act, Recital 53)
		Does the AI system only perfom a series of narrow procedural tasks?	(AI Act, Recital 53)

	interacting with a machine so they can make an informed decision to continue or step back.	Do you have supporting documentation that the system used falls under the category of limited risk?	(AI Act, Recital 53)
	General Purpose AI Models: An AI model, including one 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 the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This excludes AI models that are used for research, development or prototyping activities before they are placed on the market.	Is your AI system considered a general purpose AI model?	(AI Act, art. 3, recitals 97, 98, 99)
	General Purpose AI Models with Systemic Risk A general-purpose AI model shall be classified as a general-purpose AI model with systemic risk if it meets any of the following conditions: (a) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks; (b) based on a decision of the Commission, ex officio or following a qualified alert from the scientific panel, it has capabilities or an impact equivalent to those set out in point (a) having regard to the criteria set out in Annex XIII.	Is your AI system considered a general purpose model with systemic risk?	(AI Act, art. 51)
	Risk classification: Unacceptable, high, medium or low risk AI systems	Have you determined how your AI system is classified under the EU AI Act?	(AI Act, art. 6-8)
	Requirements for High-Risk AI Systems		
	Data Governance and Quality	To the extent possible, have you verified the quality of the dataset you are using to ensure it is accurate and does not perpetuate bias?	(AI Act, art. 10)
		To the extent possible, have you established governance mechanisms to ensure that the dataset you are using is accurate and does not perpetuate bias?	(AI Act, art. 10)

	Transparency	Have you informed all relevant stakeholders that they are interacting with an AI system? Including employees, teachers and students?	(AI Act, art. 13)
Artificial Intelligence Act (AI Act)		Are you transparent about how the AI system operates and what its limitations are?	(AI Act, art. 13)
		Are you transparent about the extent to which AI systems influence decision-making?	(AI Act, art. 13)
	Human Oversight	Are there mechanisms in place to ensure sufficient human oversight in the quality and accuracy of AI system outputs?	(AI Act, art. 14)
		Are there mechanisms in place to ensure human intervention to avoid AI-related errors, harms, risks and incidents throughout the duration of its use?	(AI Act, art. 14)
	Accuracy, Robustness, and Security	Have you assessed the AI system for threats or errors that could negatively impact users of the system?	(AI Act, art. 15)
		Does the AI system adhere to relevant accuracy, robustness, and cybersecurity standards?	(AI Act, art. 15)
	Record-keeping	If your AI system is high-risk, are you maintaing logs of the system's activities? Including inputs, outputs, and decision-making consistently?	(AI Act, art. 12)
		Are you able to maintain logs of the system's activities for its entire duration of use?	(AI Act, art. 12)
	Obligations of Providers* of High-Risk AI Systems		
	Providers of high-risk AI systems	(a) ensure that their high-risk AI systems are compliant with the requirements set out in Section 2; (b) indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted; (c) have a quality management system in place which complies with Article 17; (d) keep the documentation referred to in Article 18; (e) when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19;	(AI Act, art. 16 and recital 80)

		(f) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43, prior to its being placed on the market or put into service; (g) draw up an EU declaration of conformity in accordance with Article 47; (h) affix the CE marking to the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, to indicate conformity with this Regulation, in accordance with Article 48; (i) comply with the registration obligations referred to in Article 49(1); (j) take the necessary corrective actions and provide information as required in Article 20; (k) upon a reasoned request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Section 2; (l) ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.	
	Conformity Assessments For high-risk AI systems referred to in points 2 to 8 of Annex III, **providers** shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body.	Are you the **provider** of a high-risk AI system subject to a conformity assessment?	(AI Act, art. 43)
		If so, have you performed a conformity assessment?	(AI Act, art. 43)
		If so, have you submited the pre-market conformity assessment to the notifying authority?	(AI Act, art. 43)
	Using AI systems in Accordance with Instructions for Use Deployers of high-risk AI systems shall take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems, pursuant to paragraphs 3 and 6.	Have you or the designated person taken appropriate technical and operational measures to ensure that the AI System is used in accordance to its instruction for use?	(AI Act, art. 26)
		Have you made any significant modifications or alterations to the AI system that are not in aligenment with the instructions of use for the AI system?	(AI Act, art. 26)

		Have monitoring mechanisms been established for ensuring the continuation of measures that ensure the AI system is used in accordance with its instructions for use?	(AI Act, art. 26)
		Could users (teachers, administrators, students) misuse the AI system in a way that would make it incompatible with its instruction for use?	(AI Act, art. 26)
	Reporting serious incidents and malfunctions **Deployers** shall monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72. Where deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk within the meaning of Article 79(1), they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system.	In the case that the high risk AI system is used in accordance with its instruction of use and may result in a risk (ref. Art. 79), have you notified the provider and the relevant market surveillance authority?	(AI Act, art. 26)
		In the case that the high-risk AI system is used in accordance with its instruction of use and may result in a risk, are you prepared to suspend the use of that system?	(AI Act, art. 26 and 79)
		Are there measures in place to continuously monitor and check for incidents for the duration of the AI system's use?	(AI Act, art. 26)
Artificial Intelligence Act (AI Act)	Where **deployers** have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. If the deployer is not able to reach the provider, Article 73 shall apply mutatis mutandis.	Should a serious incident occur, are you able to properly identify and notify the relevant stakeholders (i.e., relevant institutional authority, provider, market surveillence authority)?	(AI Act, art. 26)
	Ensure Human Oversight **Deployers** shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support.	Has someone in your organisation been appointed to provide human oversight of AI systems?	(AI Act, art. 26)
		Does the designated person have sufficient competence, training, authority, and support to oversee the use of high-risk AI systems at your organisation?	(AI Act, art. 26)
		Are they aware of your intention to use a high-risk AI system in you work?	(AI Act, art. 26)
	Data Quality The extent the deployer exercises control over the input	Do you or someone at your organisation exercise control over the input data?	(AI Act, art. 26)

	data, that **deployer** shall ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system.	If so, have you or that person taken steps to ensure that the input data is relevant and sufficiently representative for its intended purpose?	(AI Act, art. 26)
	Record-keeping and Logs **Deployers** of high-risk AI systems shall keep the logs automatically generated by the high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in an applicable Union or national law, in particular in the Union law on the protection of personal data.	Are you able to keep logs automaticially generated by the AI system?	(AI Act, art. 26)
		Are you able to keep these logs for the duration of intended use of the AI system?	(AI Act, art. 26)
	Notification of use of high-risk AI system Before putting into service or using a high-risk AI system at the workplace, **deployers** who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. This information shall be provided, where applicable, in accordance with the rules and procedures laid down in Union and national law and practice on information of workers and their representatives.	Have measures been put in place to ensure that all affected persons are aware that they may be subject to the use of a high-risk AI system? Including employees, students, teachers, etc.	(AI Act, art. 26, recital 92)
	Use of AI for decision making Without prejudice to Article 50 of this Regulation, **deployers** of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system. For high-risk AI systems used for law enforcement purposes Article 13 of Directive (EU) 2016/680 shall apply.	Is the AI system being used to make decisions or assist in making decisions related to other individuals?	(AI Act, art. 26)
		If so, have you notified affected individuals that they are subject to the output of a high-risk AI system?	(AI Act, art. 26)
	Documentation **Deployers** of high-risk AI systems that are public authorities, or Union institutions, bodies, offices or agencies shall comply with the registration obligations referred to in Article 49. When such deployers find that the high-risk AI system that they envisage using has not been registered in the EU database referred to in Article	Have you registered your institution and the AI system in the EU database before beginning to use the AI system?	(AI Act, art. 26)

	71, they shall not use that system and shall inform the provider or the distributor.		
	Fundamental Rights Impact Assessments (FRIA) Prior to deploying a high-risk AI system deployers that are bodies governed by public law, or are private entities providing public services, and **deployers** of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce. For that purpose, deployers shall perform an assessment consisting of: (a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose; (b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used; (c) the categories of natural persons and groups likely to be affected by its use in the specific context; (d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13; (e) a description of the implementation of human oversight measures, according to the instructions for use; (f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.	Are you the **deployer** of a high-risk AI system subject to a FRIA?	(AI Act, art. 27)
		If yes, are you considered a **deployer** that are bodies governed by public law, or are private entities providing public services?	(AI Act, art. 27)
		If yes, have you performed a FRIA prior to deploying the AI system?	(AI Act, art. 27)
		If applicable, is your FRIA complentary to your DPIA?	(AI Act, art. 27)
		Have you submited your FRIA to the relevant bodies/authorities? Including the notifying body (pre-market), and the National Surveillence Authority (post-market)	(AI Act, art. 27)
IP Rights	Two specific issues arise from the interaction between copyright and generative AI, which can be divided into two main categories: - The potential copyright infringement by the developers of these generative AI tools, through the use of	Ownership of Generated-AI related content: the providers, the company or institution that has the licence, the users?	(32)
		Use of copyright-protected materials to train an algorithm part of an AI Model (such as LLMs)	

	copyright-protected materials to train their algorithms. This data is collected through techniques known as "mining". - Whether works produced by – or with – generative AI tools are copyright-protected, and who owns the resulting copyright?	GenAI references and citation, how to refer to AI Systems content generated?	(33)

References

Bozkurt, A. (2024). GenAI et al.: Cocreation, Authorship, Ownership, Academic Ethics and Integrity in a Time of Generative AI (1). 16(1), Article 1. https://doi.org/10.55982/openpraxis.16.1.654

Commonwealth of Australia. (2024). Australian Framework for Generative Artificial Intelligence in Schools. https://www.education.gov.au/schooling/resources/australian-framework-generative-artificial-intelligence-ai-schools

Directorate-General for Education, Y. (2022). Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators. Publications Office of the European Union. https://data.europa.eu/doi/10.2766/153756

Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.8cd550d1

Hardebolle, C., Macko, V., Ramachandran, V., Holzer, A., & Jermann, P. (2023). Digital Ethics Canvas: A Guide For Ethical Risk Assessment And Mitigation In The Digital Domain. https://doi.org/10.21427/9WA5-ZY95

High-Level Expert Group on AI. (2019, April 8). Ethics guidelines for trustworthy AI | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Holmes, W. (2024). AI, AIED and Human Agency. https://pressbooks.pub/aiforteachers/chapter/ai-aied-and-human-agency/

Holmes, W., Fengchun, M., & UNESCO. (2023). Guidance for generative AI in education and research. UNESCO Publishing.

Holmes, W., Porayska-Pomsta, K., Holstein, K., Sutherland, E., Baker, T., Shum, S. B., Santos, O. C., Rodrigo, M. T., Cukurova, M., Bittencourt, I. I., & Koedinger, K. R. (2022). Ethics of AI in Education: Towards a Community-Wide Framework. International Journal of Artificial Intelligence in Education, 32(3), 504–526. https://doi.org/10.1007/s40593-021-00239-1

Holmes, W., Persson, J., Chounta, I.-A., Wasson, B., & Dimitrova, V. (2022). Artificial intelligence and education: A critical view through the lens of human rights, democracy and the rule of law. Council of Europe.

Holmes, W., Bialik, M., & Fadel, C. (2019). Artificial intelligence in education: Promises and implications for teaching and learning. The Center for Curriculum Redesign.

Ruttkamp-Bloem, E. (2020). The Quest for Actionable AI Ethics. In A. Gerber (Ed.), Artificial Intelligence Research (Vol. 1342, pp. 34–50). Springer International Publishing. https://doi.org/10.1007/978-3-030-66151-9_3

Sahlgren, O. (2023). The politics and reciprocal (re)configuration of accountability and fairness in data-driven education. Learning, Media and Technology, 48(1), 95–108. https://doi.org/10.1080/17439884.2021.1986065

Selwyn, N. (2023). AI, education, and ethics—Starting a conversation. In W. Holmes & K. Porayska-Pomsta (Eds.), The ethics of artifical intelligence in education: Practices, challenges, and debates. Routledge.

Şenocak, D., Bozkurt, A., & Kocdar, S. (2024). Exploring the Ethical Principles for the Implementation of Artificial Intelligence in Education: Towards a Future Agenda (pp. 200–213). https://doi.org/10.4018/979-8-3693-1351-0.ch010

UNESCO. (2021). AI and education: Guidance for policy-makers. UNESCO. https://doi.org/10.54675/PCSP7350

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU law: liability, privacy, intellectual property, and cybersecurity. arXiv preprint arXiv:2401.07348.

Kloos, C. D., Alario-Hoyos, C., Estévez-Ayres, I., Callejo-Pinardo, P., Hombrados-Herrera, M. A., Muñoz-Merino, P. J., ... & Ibáñez, M. B. (2024, May). How can Generative AI Support Education?. In 2024 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-7). IEEE.

Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems: 24-05-29_genai_orientations_en_0.pdf (europa.eu)

Living guidelines on the responsible use of generative AI in research: 2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en (europa.eu)

Guidelines on the Use of Digital Tools in Education from a Data Protection Perspective: Guidelines on the use of Digital Tools in Education from a Data Protection Perspective (intef.es)

The impact of the General Data Protection Regulation (GDPR) on artificial intelligence: EPRS_STU(2020)641530_EN.pdf (europa.eu)

Generative AI: The Data Protection Implications : generative-ai-the-data-protection-implications-16-10-2023.pdf (cedpo.eu)

THE STATE OF ARTIFICIAL INTELLIGENCE AND EDUCATION ACROSS EUROPE 1680aef139 (coe.int)

AI system development: CNIL's recommendations to comply with the GDPR: AI system development: CNIL's recommendations to comply with the GDPR | CNIL

License used: This work is licensed under a Creative Commons Attribution Share Alike 4.0 International License: https://creativecommons.org/licenses/by-sa/4.0/
With this license, you are free to **share** copy and redistribute the material in any medium or format. You can also **adapt** remix, transform and **build upon** the material for any purpose, even commercially.

But only Under the following terms:
Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. **Share Alike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

Co-funded by
the European Union