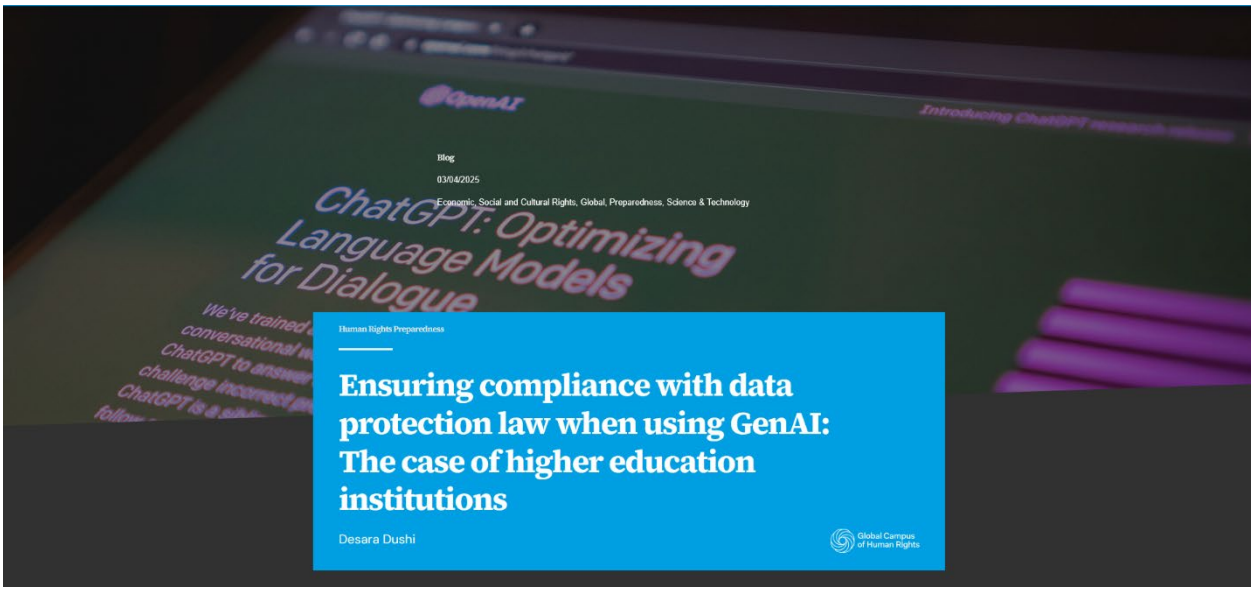

Ensuring compliance with data protection law when using GenAI: The case of higher education institutions

Desara Dushi*

Abstract: European universities using GenAI, such as ChatGPT, for administrative services must comply with the General Data Protection Regulation. This includes managing personal data carefully, ensuring transparency, and adhering to principles like data minimisation and accuracy to protect privacy and uphold students' rights.

European universities can develop and deploy their own generative AI solutions or alternatively use market-available solutions like ChatGPT for their administrative services. This includes offering a chatbot service to students for quicker and more simplified explanations of rules for both current and incoming students. If the use of ChatGPT involves the processing of personal data, the General Data Protection Regulation (GDPR) applies.

* Dr. Desara Dushi is a senior postdoctoral researcher at the Law, Science, Technology & Society Research Group (LSTS), Vrije Universiteit Brussel. She holds a double PhD degree in Law, Science and Technology from University of Bologna and University of Luxembourg. She is one of the policy analysts of the 6th edition and Global Campus Policy Observatory.

GDPR applies to all personal data processing activities, regardless of the technologies used, and without prejudice to other legal frameworks, such as the AI Act. The GDPR's accountability principle requires that the responsibilities amongst the various actors involved in the generative AI model supply chain be clearly identified and respected. As a first step, higher education institutions (HEIs) must explicitly determine their role as controller, processor, or joint controllership, when deciding to use a GenAI system.

Does the use of GenAI involve personal data processing?

The short answer is yes. Personal data can be processed at different stages, specifically: at the training dataset (since OpenAI's models are trained on data scraped from the internet, which likely includes some personal information, even if it is publicly available); at the training stage (from the HEIs' own files); from individuals' interactions with the system through the inputs they provide; and even from the outputs generated by the system.

When deciding to use ChatGPT for their services, HEIs need to restrict what student data and personal information can be input into the GenAI tools they deploy to mitigate privacy risks. To ensure there is no processing of personal data in cases where the model is not intended for it, universities deploying their own GenAI tools, as well as those using ChatGPT, should conduct regular monitoring and implement controls at all stages, collaborating with OpenAI in the latter case.

ChatGPT is a general-purpose model, not a domain-specific model. However, it can be fine-tuned for specific domains. To achieve this, HEIs would need to collaborate with OpenAI by providing training data and datasets from universities to help fine-tune the model for the needs of HEIs.

Moreover, HEIs should keep in mind that, regardless of the accuracy and appropriateness of the training data, ChatGPT may still hallucinate by fabricating facts and producing output not supported by the source material.

This is because, like all systems built on Large Language Models (LLMs), ChatGPT's output relies on next-word prediction rather than reasoning or understanding. This could be concerning if such a system is used to provide simplified information to students about rules, administrative procedures, and assistance, potentially leading students to depend on inaccurate information.

Lawfulness of personal data processing

The processing of personal data must be based on one of the legal grounds outlined in Article 6 of the GDPR, such as the consent of the data subjects or the performance of a task carried out in the public interest. Consent should be obtained in an informed and voluntary manner.

Therefore, when deciding to implement ChatGPT in their administrative processes, HEIs must ensure that the processing of special categories of data by the tool complies with specific exceptions outlined in Article 9(2) of the GDPR. Additionally, all necessary protective measures must be taken to safeguard individuals' right to the protection of personal data, particularly data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and health-related information, as well as a person's sexual life or orientation. This is also enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 2 of the International Covenant on Economic, Social and Cultural Rights (ICESCR), and Article 8 of the European Convention on Human Rights (ECHR).

The principle of data minimisation

The principle of data minimisation (under Article 5(1)(c) of the GDPR) requires that personal data processed be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. This obligation also applies to the entire lifecycle of the GenAI system. Therefore, ChatGPT must limit the collection and processing of personal data to what is strictly necessary. Moreover, it is crucial to adopt anonymization and pseudonymisation techniques wherever possible to further mitigate privacy risks.

The principle of data accuracy

The data accuracy principle, as outlined in Article 5(1)(d) of the GDPR, mandates that personal data must be accurate and kept up to date. Therefore, ChatGPT must integrate data protection by design to minimise the risk of errors and ensure the reliability of the data used.

Higher education institutions integrating GenAI into their systems must secure contractual assurances and documentation regarding the procedures used to ensure the accuracy of the data employed in the system's development. This is crucial because GenAI can generate outputs containing inaccurate or false information, including personal data, referred to as 'hallucinations', which may affect students' fundamental rights, such as the right to accurate information. It also impacts the right to privacy, as incorrect or mishandled personal data can lead to violations of privacy rights.

Privacy by design and by default

GenAI systems are evolving rapidly. For example, ChatGPT, which previously accepted only text, has now become multimodal and accepts various types of input. This presents new risks to the fundamental rights and freedoms of its users, such as the right to privacy and data protection. The creation of deepfake videos that fabricate harmful or

embarrassing scenarios misrepresenting individuals also impacts personal dignity, damaging their reputation and integrity while causing emotional distress.
This is why the principle of privacy by design and by default (Article 25 of the GDPR) requires developers, providers, and deployers of GenAI systems to conduct a data protection and privacy impact assessment. This assessment helps identify, assess, and address the risks posed by these systems at every stage of their life cycle, starting from the design stage and continuing after every modification or fine-tuning.

How can students be informed about how personal data is processed when HEIs use GenAI systems?

Another important aspect is the obligation to adequately inform individuals about the processing of their personal data. HEIs must ensure that students and prospective students understand that their data is being processed, the purposes of that processing, and their rights regarding the data, including informing them that they are interacting with a GenAI system. This includes providing clear and accessible information that complies with GDPR requirements.
In this regard, HEIs should create and uphold transparency and communication policies that outline how data is collected, used, and stored. This information must be consistently updated to reflect any changes in data processing practices.
Furthermore, when using AI systems that make automated decisions, such as assessing entry qualifications, it is essential to explain the logic behind these decisions and the possible consequences for students and prospective students, ensuring they have the right to contest such decisions.