



ARTICLE

AUTHOR: **LAURA DRECHSLER**

KU LEUVEN

The GDPR as the building code for AI-systems

Artificial Intelligence (AI) has entered our daily lives – or at least our news-feeds. Each day brings new promises about how AI will either enhance society or destroy life as we know it (or potentially both). In the world of EU law, the growing interest in the various potential applications of AI is reflected in the increasing publication stream on the AI Act – a product safety regulation with a fundamental rights dimension, adopted by the EU in 2024 and now gradually entering into force. What is sometimes overlooked in the intense preparations for the full implementation of the AI Act is that AI is already subject to an existing and fully appli-

The GDPR should not be seen as a barrier to innovation, but rather as a safeguard to ensure that the fundamental rights at the heart of the EU legal order are not abandoned in the name of technological progress.”

cable legal framework: the General Data Protection Regulation (GDPR). In this essay, I examine the role of the GDPR in the development of AI systems, positioning it as a 'building code' that must be respected by all technologies – including AI – that rely on personal data.

Moving from personal data to data protection principles.

The GDPR applies to the use of personal data, which is defined as any information that can make a person identifiable (Article 4(1)). The Court of Justice of the EU (CJEU) has interpreted this definition broadly to ensure comprehensive protection for individuals. It has, for example, ruled that dynamic IP addresses, TC strings, exam results, and Google search results can all constitute personal data. This broad conceptualization makes it likely that AI systems will use personal data at some point between the training phase and the deployment of the system in a specific use case. This is particularly true because anonymization remains notoriously difficult and unstable.

As more data becomes available online, the risk of re-identification increases, making anonymization techniques more fragile. Ongoing discussions about whether specific stages of the AI lifecycle involve personal data – such as whether the AI model itself qualifies as personal data – arguably miss the point and risk diverting attention from the pressing question: how can AI systems comply with the core principles of the GDPR, as clearly set out in Article 5? These include lawfulness, fairness, transparency, purpose specification, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

These principles – sometimes referred to as the “ten commandments” of EU data protection law – were not invented by the GDPR. Rather, they are rooted in regulatory thinking that dates back to the late 1970s and early 1980s, both in Europe and beyond. The concerns that motivated their development sound eerily familiar: the rapid introduction of new technologies (back then computers and central databases)

and fears of surveillance by both public authorities and the private sector (through practices such as credit scoring).

Even AI – albeit more as a theoretical concept – was already being discussed and eventually found its way into the 1995 Data Protection Directive, the GDPR's predecessor, with specific rules on automated decision-making.

Data protection principles as design requirements

The data protection principles have always functioned as design requirements for any system that uses personal data – a point made even more explicit with the introduction of data-protection-by-design and by-default in Article 25 of the GDPR. In this sense, the principles can be seen as the EU's “building code” for technologies, including AI systems targeting EU residents. Building codes set out rules for how physical structures must be constructed to meet safety, health, and environmental standards. Crucially, as any good architect knows, building codes must be considered from the very beginning of the design process. They define the outer limits of what building design can achieve, while leaving ample room for innovation within those boundaries. Enforcement is strict – after all, no one wants to live in a world with unstable or unsafe buildings. In cases of serious violations, enforcement may even include the dismantling of existing structures.

The GDPR as AI's building code

Normatively, the GDPR's principles should be treated in the same way as a building code. They define the outer boundaries of what technologies – such as AI – may do with personal data to safeguard fundamental rights and freedoms established in the EU Charter. These principles are deliberately abstract and open-ended, allowing room for innovation within those boundaries. However, they must be carefully considered before unleashing AI on EU residents. Enforcement should be strict and, in extreme cases, may even require the deletion of data sets or the banning of certain technologies (as exemplified by the

temporary actions taken by the Italian data protection authority against ChatGPT and DeepSeek). The GDPR's adoption of a risk-based approach should not be interpreted as a signal that its principles are negotiable. Rather, this approach determines the scope within the established boundaries – granting more flexibility where the risks are lower. Similarly, building codes become stricter when buildings pose greater risks, for example due to their height, location, or function.

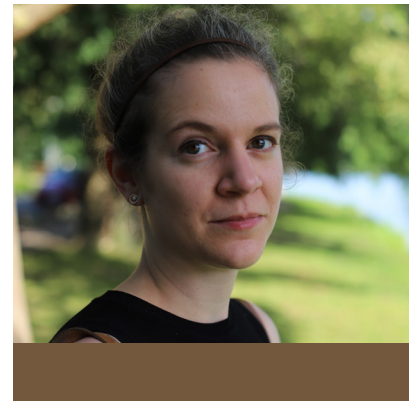
Conclusion

The role of the GDPR as a building code for all technologies, including AI systems that use personal data, complements the approach of the AI Act, which imposes additional requirements based on the risk posed by a given system. The GDPR thus serves as a baseline as it applies regardless of the AI Act's risk classification. As such, it must be a key legal consideration from the very beginning of AI system and model design. It should not be seen as a barrier to innovation,

but rather as a safeguard to ensure that the fundamental rights at the heart of the EU legal order are not abandoned in the name of technological progress.

Moreover, data protection regulators should not hesitate to hold actors accountable for failing to follow the code, taking a cue from the Italian authority. If we aim to live in a world where the GDPR is a lived reality, we must support those who take the time to understand and comply with its principles – not those who prioritize speed over safeguards. After all, Move fast and break things was never sound legal advice.

About the author: Laura Drechsler is Assistant Professor for data law at the Centre for IT and IP Law (CiTiP) at the KU Leuven and the State Archives of Belgium. She is also a lecturer in data protection law at the Open Universiteit in Heerlen. Her research focuses on the intersection of EU data protection law with EU data legislation from a human rights perspective.



“

MOVE FAST AND BREAK THINGS WAS

NEVER SOUND LEGAL ADVICE

”