AI and GDPR: A tight affair

April 20, 2022

Introduction

This time last year, the European Union took a decisive first step in the direction of regulating lawful, safe and trustworthy artificial intelligence technologies by publishing the so-called AI Act—officially known as the "Proposal for a Regulation laying down harmonized rules on Artificial Intelligence." The AI Act represents a crucial opportunity for the European Union to ensure that AI systems operating in the single market respect the EU's fundamental rights and values. Some commentators anticipated that the AI Act may lead the European Union to once again become a standards-setter on the international scene, similarly to what happened with regards to the General Data Protection Regulation (GDPR).

There are, in fact, a number of **common features between the AI Act and the GDPR**. This did not come up as a surprise: on the one hand, the right to protection of personal data is considered a fundamental right within the EU's legal framework, by both article 16 of the Treaty on the Functioning of the European Union and article 8 of the EU's Charter of Fundamental Rights. On the other hand, data is to AI what fuel is to an engine. We all know that training AI systems requires a massive amount of data (including personal data), thus rendering data protection law relevant when regulating this new family of technologies.

To celebrate the first anniversary of the AI Act, we address here the main similarities shared with the GDPR, such as the **scope of application**, the **risk-based approach**, the **accountability principle**, the **risk management system**, and **administrative sanctions**. Then, we will look into the envisaged governance system at both the EU and national levels, focusing in particular on the designation of a national supervisory authority.

Common points between the AI Act and the GDPR

1. Scope

Looking at article 2 of the AI Act, the first feature borrowed from the GDPR is in fact the **extensive scope of application**, well beyond European "borders." Indeed, three categories of subjects will be bound by these provisions: not only users of AI systems located within the territory of a member state but also providers that place AI systems on an EU market or put them into service in the EU, irrespective of whether they are established in the EU. Furthermore, third-country providers and users of AI systems will fall within the scope of application if the output generated by such systems is used in the EU.

2. Risk-based approach

A key point of the GDPR is the innovative risk-based approach, which requires the data controller to consider "the nature, scope, context and purposes of processing, as well as the risks for data subjects' rights and freedoms" in

order to implement technical and organizational measures compliant with the GDPR. In other words, the controller is responsible for detecting the specific issues of the processing activities carried out and then for addressing them with the means it deems appropriate. **The AI Act adopts a similar risk-based approach** that, besides serving compliance purposes also drives the categorization of AI systems into four different families, based on the degree of risk posed to individuals' fundamental rights and freedoms. The "risk ladder" is the following: **unacceptable-risk AI systems** are expressly prohibited; **high-risk AI systems** are subject to mandatory requirements and an ex-ante conformity assessment; **limited risk AI systems** are only subject to specific transparency obligations, while **minimal risk AI systems** that fall outside the scope of regulation can be freely used.

3. Accountability

The GDPR provides for the data controller to be responsible for—and be able to demonstrate compliance with—th safeguarding principles relating to the processing of personal data. **The AI Act, although not specifically mentioning the accountability principle, extends this principle to all operators involved in the supply chain**. For instance, Chapter 3 of the AI Act, which deals with enforcement, places horizontal obligations on providers of high-risk AI systems, but also establishes proportionate obligations for users and other players within the AI value chain, such as importers, distributors and authorized representatives.

4. Risk management

Article 9 of the AI Act regulates the establishment, implementation and documentation of a risk management system, which needs to be properly managed throughout the entire life cycle of high-risk AI technologies. This mechanism is described as a continuous process aimed at identifying the foreseeable risks of high-risk AI systems—as well as other possible threats arising from post-market monitoring data—and suitable measures to manage all these risks.**Such risk management system is aligned with the data protection impact assessment provided for in article 35 GDPR** —which basically requires data controllers to previously assess the impact of a processing activity on the protection of personal data.

5. Sanctions

The GDPR and AI Act provides for similar types of administrative fines. First, for "minor infringements" fines can be imposed of up to €10 million or 2 percent of the total annual global turnover of the preceding financial year, whichever is higher. Such infringements include, for instance, for the GDPR violating the principle of privacy by design and by default, and for the AI Act for providing incorrect, incomplete or misleading information to notified bodies and national authorities. Fines can then be raised to €20 million or 4 percent of the total annual turnover of the preceding financial year for breaching other provisions of the GDPR, such as processing principles and data subjects' rights, or for other violations of the AI Act that do not fall within the lower level of fines. Finally, the AI Act adds another (and more severe) layer of fines, up to €30 million or 6 percent of the total annual turnover of the preceding financial year whichever is higher, for non-compliance with prohibited AI practices or the quality requirements set out for high-risk AI systems.

6. Oversight

As for monitoring and enforcement, **both regulations identify a similar oversight mechanism** that relies on the cooperation of European and national authorities in order to ensure consistent and effective application of the

regulation.

On the European level, article 68 of the GDPR established the European Data Protection Board (EDPB), which comprises the heads of the national supervisory authorities and of the European Data Protection Supervisor (EDPS); in addition, the European Commission has the right to participate in its activities. Following the same path, articles 56 and 57 of the AI Act lay the foundations for the European Artificial Intelligence Board, a new body that, similarly to the EDPB, comprises representatives from the member states and the EDPS. In this case, however, the Commission enjoys a more prominent role by chairing the board, convening the meetings and preparing the agenda.

On a national level, article 51 of the GDPR prompts member states to identify one or more supervisory authority that will be responsible for monitoring data protection regulations. In the same way, article 59 of the AI Act requires each member state to establish or designate national competent authorities for the purpose of guaranteeing proper application of the regulation. In both cases, such authorities are subject to strict requirements of independence, objectivity and impartiality, and it is furthermore up to each member state to provide their authority(ies) with the adequate financial, technical and human resources to fulfil their tasks.

Scholars and lawyers are divided as to which authorities should be identified as national competent authorities. **A number of commentators (e.g. including the EDPB and the EDPS in their joint opinion 05/2021) support extending this function to national data protection authorities (DPAs)**. Such solution could be justified for the following main reasons: (i) these authorities already exist, so no additional costs are necessary to put into place a new regulatory body; (ii) since data protection and artificial intelligence are deeply intertwined, granting the supervisory role to a single subject would ensure a uniform and effective action in these two fields—by contrast, establishing a new body may lead to coordination problems; and (iii) as the AI Act borrows numerous features from the GDPR, the national DPAs would be already accustomed to the approaches and tools that are intended to be used.

The future of the AI Act

Whether the AI Act will set the conditions for the EU to become a global (regulatory) trend setter is yet to be determined. Much will also depend upon the concrete technological and economical leadership that will be exercised by the EU, as well as whether the AI Act is in actuality applied uniformly within the EU member states. In this respect, certain commentators pointed out that the AI Act may leave room for discretion in adapting the regulation to national frameworks. The debate is therefore still very open. There is, however, an increasing consensus among commentators for regulations that, like the AI Act, aim at setting a common level playing field, allowing operators from different jurisdictions to exploit new technologies with a humancentric approach.

Luca Zannoni (luca.zannoni@dentons.com), **Marco Propato** (marco.propato@dentons.com) co-authored this article.

Your Key Contacts

Giangiacomo Olivi
Partner, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com