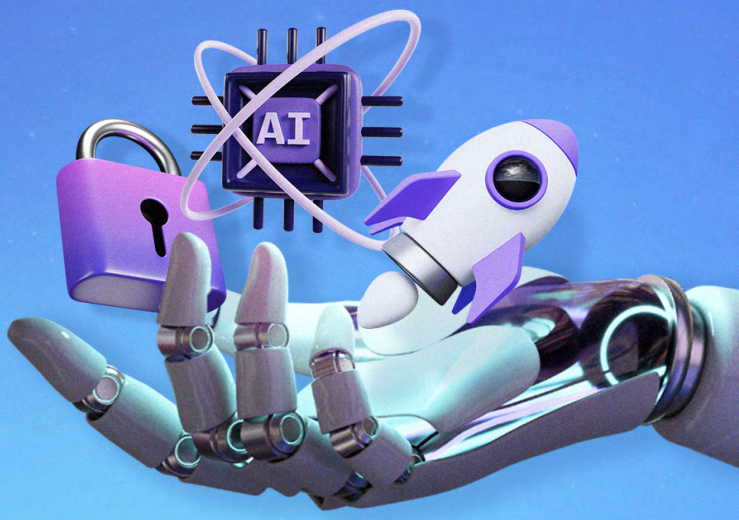
AI, Startups, and GDPR:

A Privacy Tango with a Twist



Startups are at the vanguard of providing AI solutions to grand societal challenges. Yet, those AI solutions are only as good as the data they are fed, which includes extensive amounts of personal information. This is precisely why, soon after generative AI applications like ChatGPT went viral at the end of 2022, privacy concerns rapidly became a heated topic. In this article, we will discuss how AI, startups, and privacy-related legislation interact, and address the challenges and opportunities in that space.

When startups use AI, they manage personal data in four stages: first, during the training of an algorithm; secondly, during fine-tuning; thirdly, for execution - where data is employed for prediction or classification; and finally, for ongoing monitoring and maintenance. The execution phase demands particularly careful handling as it involves applying the trained model to new data. Mishandling at this stage could lead to privacy breaches and discrimination. Startups, as AI champions, are aware of these privacy concerns and want to take the necessary steps to securely employ AI.

Unsurprisingly, the necessity to harness vast amounts of personal data alarms AI pessimists who fear an illicit use of this technology. Growing negative connotation of AI amongst citizens showcases the importance of navigating the tension between privacy and the advancement of this promising technology. Finding the right balance between the right to privacy and the need for innovation will be key to ensuring the EU remains competitive.

How are regulators across the globe addressing privacy in AI?

The European Union: The EU has positioned itself ahead of the regulatory race with the AI Act, a legislation that started with a tech-neutral and risk-based logic to govern AI systems. The final text, however, regulates

general-purpose AI models that, by definition, have no intended purpose - without specifically regulating data privacy. Data privacy is already covered by the General Data Protection Regulation (GDPR), as declared by the European Data Protection Board (EDPB): "[a]ny processing of personal data through an algorithm, falls within the scope of the GDPR." Despite this alignment in principle, tensions may arise between the AI Act and the GDPR concerning taxonomy, interpreting requirements, and other nuanced aspects, potentially creating overlaps or conflicts that need further clarification and resolution.

The United States: While the EU has taken a binding, centralised, top-down strategy to regulate AI, the US is pursuing a decentralised and bottom-up approach. This will most likely result in a patchwork of non-binding rules and guidelines, for example those suggested in the AI Risk Management Framework developed by the National Institute of Standards and Technology (**NIST**). As a reaction to the above-mentioned AI and privacy challenges, US President Joe Biden has released an **Executive Order** on the Safe, Secure, and Trustworthy Development and Use of AI, stating that US agencies shall make use of available policy and technical tools, including privacy-enhancing technologies (PETs). This highly fragmented landscape across sectors and states could be remedied through a GDPR US counterpart, the proposed American Data Privacy and Protection Act (ADPPA).

Other initiatives: Aside from the very different approaches taken by the EU and the US, other global and regional initiatives (including the OECD, the Council of Europe, etc.) have also emerged to try to tackle the same concerns. Because of the use of personal data in AI transcends borders, the international community has a shared interest in a common solution. The United Nations has created an **AI Advisory Board** with 39 experts from across the world who will base part of their work on the Universal Declaration of Human Rights, which includes the right to privacy. Meanwhile, international standardisation bodies like the International Organisation for Standardisation (**ISO**) and the International Electrotechnical Commission (**EIC**) have been working on AI standards that address privacy. In addition, the **G7** members agreed to develop an international code of conduct and guidelines, whereas, at the **G20**, privacy was deemed as necessary for ensuring responsible AI development. All of these global efforts tell us how much the international community is looking at AI and privacy, and consequently tries to spur international cooperation in AI governance.

Businesses: Policymakers aren't the only ones concerned with the privacy challenges brought by AI. For industry players, privacy regulation has created unprecedented problems for businesses, especially for startups. Indeed, while established players have the expertise to design their own technologi-

cal solutions and comply with existing rules, startups' resources are scarcer. Privacy regulation is more often than not enacted to target established players, forcing the startup ecosystem to cope with poorly-designed requirements that were not designed for them or with them. The AI Act, too, falls into the trap of replicating ideas that are supposed to hamper established or foreign companies. If one can argue that regulating privacy and AI proves challenging, the way smaller players undergo that regulation is even more challenging. For startups but also for the rest of the ecosystem, **it is therefore important to rely on existing regulations and not reinvent the wheel.**

Promoting regulatory stability: the GDPR

The GDPR, being the strongest data privacy and security law in the world, is a key reference point for addressing the complex challenges posed by AI. The GDPR was created to protect citizens' personal data while harmonising privacy rules across borders. Several overarching factors shaped its birth, including the evolving technological landscape and need for further developments of the digital single market, data breaches, and shifts in public opinion. The advancement of AI has only intensified the already exponential increase in the collection of personal data. **Fortunately, the GDPR governs the processing of data regardless of the technology employed.**

The question is how to apply the provisions of the GDPR to AI. For example, consider the 'right to erasure,' also known as the 'right to be forgotten.' In the context of AI, even in cases where it is technically feasible to erase data used for training machine learning models, doing so can have far-reaching implications. To address this and similar challenges, it is necessary to strike a balance between respecting privacy rights and enabling AI innovation. One potential solution is to integrate PETs into AI systems to anonymise personal data, as when data is not attributable to an identifiable person, it falls outside the scope of the GDPR.

Some have argued that the technological development of AI can be at odds with some of the principles of the GDPR. The 'purpose limitation' principle, which states that data must be processed for specified, explicit, and legitimate purposes, is in contradiction with the useful practice of reusing data for unanticipated purposes different from the original ones. Finding a suitable approach that permits legitimate data use while preventing privacy infringements remains a critical objective that both policymakers as well as practitioners should address jointly.

The GDPR is a technologically-neutral and principled-based law so it can be interpreted in a way that does not create unnecessary obstacles for startups to develop AI. Policymakers can consider interpretations of its provisions taking into account the unique charac-

teristics of AI applications, and contemplate the adoption of a risk-based approach that considers the benefits and risks holistically. In addition, they can provide guidelines and foster cooperation between data protection authorities and startups to ensure both privacy protection and AI innovation, such as regulatory sandboxes, or fostering cross-industry dialogue. Ultimately, when addressing the issue of privacy in AI, policymakers should begin from the premise that the GDPR does not require substantial modifications as its provisions form an adequate framework for fostering responsible data processing in AI applications.

Both the AI Act and the GDPR give citizens the right to the protection of their personal data. Avoiding a fragmented regime related to the enforcement and interpretation of the AI Act will be key. Carefully understanding how the provisions of the AI Act overlap with the GDPR is necessary to leave no room for ambiguity and confusion. In this process, startups should have a seat at the table and receive adequate guidance.

Although known for changing the world through innovation, many forget that startups' resources are often limited. Having faced many challenges complying with the GDPR, today they are presented with an opportunity. The well-established data processing basis and principles of the GDPR provide a solid framework to regulate privacy in AI. This will create more legal certainty and foster a more supportive environment for startups already familiar with the GDPR. By crafting regulations that these small but mighty actors can comply with, we ensure the growth of a safe and innovative ecosystem so that the EU can be at the vanguard of disruption and build its own technological giants.