COMPLIANCE WEEK

{REGULATORY POLICY}

What you need to know about proposed EU rules for trustworthy AI

BY NEIL HODGE

The European Commission last week unveiled proposals to ensure trust in the use of artificial intelligence (AI)—not just for Big Tech, but for all companies that use the technology.

The proposed rules will apply to both the developers and users of AI and will have an extraterritorial reach if the AI system is used in the European Union or affects people located in the single market.

The Commission proposed a risk-based approach in terms of oversight, with four risk levels: unacceptable, high, limited, and minimal.

Any AI technology that poses an unacceptable risk to consumers and/or violates fundamental rights will be automatically banned. Examples include the exploitation of vulnerabilities of children, the use of subliminal techniques (such as behavioral advertising), credit scoring, and the use of live remote biometric identification systems in public places.

High-risk AI systems are determined by—among other issues—how many individuals might be affected by the technology's use, the dependency of the outcome, and the level of harm that could be caused by the decisions/information generated.

As such, high-risk systems will mandate stricter compliance requirements, which will cover the quality of data sets used; technical documentation and record keeping; transparency and the provision of information to users; human oversight; and robustness, accuracy, and cyber-security. In case of a breach, the requirements will allow national authorities to have access to the information needed to investigate whether the use of the AI system complied with the law.

Prior to launching high-risk products and services, developers will need to pass a conformity assessment to see if they meet the EU's criteria for trustworthy AI. If the system is "substantially" modified, it would need to undergo another assessment before being made available.

AI systems with limited risks will likely have to comply with specific transparency requirements. For example, if people are engaging with chatbots rather than humans, users should be aware they are interacting with a machine.

Minimal-risk AI systems—which constitute the vast majority—can be developed and used without additional legal obligations. However, providers of those systems may voluntarily choose to apply the EU's proposed requirements for trustworthy AI and adhere to voluntary codes of conduct.

> "Organizations should already be doing a lot of the work envisaged by the new regulation as part of their data protection impact assessments."
>
> Camilla Winlo, Director of Consultancy, DQM GRC

The regulation will be enforced similar to the General Data Protection Regulation (GDPR): Each EU member state will designate one or more national competent authorities to supervise its application and implementation, as well as carry out market surveillance activities. These designated authorities will also be part of a planned European Artificial Intelligence Board aimed at harmonizing enforcement decisions across the bloc (like the European Data Protection Board does with the GDPR).

And, like the GDPR, the proposed penalties are steep. There are three categories of sanctions:

1. Up to €30 million (U.S. $36.3 million) or 6 percent of the total worldwide annual turnover of the preceding financial year (whichever is higher) for infringements on prohibited practices or noncompliance related to requirements on

data.
2. Up to €20 million (U.S. $24.2 million) or 4 percent of the total worldwide annual turnover of the preceding financial year for noncompliance with any of the other requirements or obligations of the regulation.
3. Up to €10 million (U.S. $12.1 million) or 2 percent of the total worldwide annual turnover of the preceding financial year for the supply of incorrect, incomplete, or misleading information to notified bodies and national competent authorities in reply to a request.

There is still a long way to go before the regulation—or something resembling it—is enacted. The proposed rules first need to be adopted by the European Parliament and member states, which means they can be modified. Given EU governments will then have two years to enact the legislation, the earliest possible date it could come into force will be 2023.

Experts say the regulation shows the EU's intent. Further, many believe it might be a step in the right direction and that the compliance requirements may not be overly onerous.

Camilla Winlo, director of consultancy at data management specialist DQM GRC, says the proposals are "an extension and clarification of what is already necessary rather than a completely new set of requirements." She adds, "Organizations should already be doing a lot of the work envisaged by the new regulation as part of their data protection impact assessments."

Peter van der Putten, assistant professor of AI at Leiden University in The Netherlands, also believes the Commission's proposals are not as radical as companies may initially think. "These kinds of policies will be setting broad boundary conditions only," he says. He expects the rules will produce a shift toward "mutually beneficial AI" as "consumers will vote with their feet if they don't feel there is a win-win for both parties."

Alex van der Wolk, partner in the privacy and data security practice at law firm Morrison & Foerster, says one drawback might be that the threshold for what qualifies as AI is "extremely low"—so much so that "most data analytics and query tools will be required to meet this regulation." ■