Volume 5, No. 2 | March–April 2022

The Journal of Robotics, Artificial Intelligence & Law

European Commission's Proposed Regulation on Artificial Intelligence: Conducting a Conformity Assessment for High-Risk AI—Say What?

Karen L. Neuman, Dorothy Cory-Wright, Colleen B. Hespeler, and Madeleine White

fastcase FULL COURT PRESS

European Commission's Proposed Regulation on Artificial Intelligence: Conducting a Conformity Assessment for High-Risk AI—Say What?

Karen L. Neuman, Dorothy Cory-Wright, Colleen B. Hespeler, and Madeleine White*

This article summarizes the requirements for conducting a conformity assessment, including unique considerations that apply to data-driven algorithms and outputs that typically have not applied to physical systems and projects under EU product safety legislation; discusses the potential impacts of this new requirement on the market and how it will fit within the existing sectoral safety legislation framework in the European Union; and identifies some strategic considerations, including in the context of product liability litigation, for providers and other impacted parties.

The European Commission ("EC") on April 21, 2021, proposed a regulation establishing a framework and rules ("Proposed Regulation") for "trustworthy" artificial intelligence ("AI") systems. The Proposed Regulation aims to take a proportionate, risk-based regulatory approach by distinguishing between "harmful" AI practices, which are prohibited, and other AI uses that carry risk, but are permitted. These uses are the focus of the Proposed Regulation: high-risk AI systems can only be placed on the EU market or put into service if, among other requirements, a "conformity assessment" is conducted prior to doing so.

This article summarizes the requirements for conducting a conformity assessment, including unique considerations that apply to data-driven algorithms and outputs that typically have not applied to physical systems and projects under EU product safety legislation, discusses the potential impacts of this new requirement on the market and how it will fit within the existing sectoral safety legislation framework in the European Union, and identifies some

Robotics, Artificial Intelligence & Law / March–April 2022, Vol. 5, No. 2, pp. 135–144.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

strategic considerations, including in the context of product liability litigation, for providers and other impacted parties.

Key Concepts

Background

The Proposed Regulation's conformity assessment requirement has its origins in EU product safety legislation. Under EU law, a conformity assessment is a process carried out to demonstrate whether specific consumer protection and product integrity requirements are fulfilled, and if not, what if any remedial measures can be implemented to satisfy such requirements. Unsafe products, or those that otherwise do not comply with applicable standards, may not make their way to the EU market. The scope of conformity assessment required differs under various directives according to the type of product and the perceived level of risk it presents, varying from self-assessment to risk assessment by a suitably qualified independent third party referred to as a "Notified Body" (whose accreditation may vary between Member States). An analogous concept in the United States is the authority of the Food and Drug Administration to require that manufacturers of medical devices follow certain regulatory procedures to market a new product in the U.S. market. The procedures required depend, among other factors, on the potential for devices to harm U.S. consumers.

As suggested, in the European Union, conformity assessments are customarily intended for physical products, such as machinery, toys, medical devices, and personal protective equipment. Examples of conformity assessments for physical products include sampling, testing, inspecting, and evaluating a product. It remains to be seen how the conformity assessments under the Proposed Regulation will work in practice when applied to more amorphous components of AI such as software code and data assets. We anticipate, however, that the focus will be on testing such systems for bias and discriminatory/disparate impacts. Factors should include ensuring that representative data are included in the models and that outcomes avoid amplifying or perpetuating existing bias or otherwise unintentionally producing discriminatory impacts, particularly where traditionally underserved populations are targeted by AI models to correct inequities (*e.g.*, an AI model might assign credit

scores to certain demographic groups that result in targeted ads for higher interest rates than advertised to other market segments).

Types of Conformity Assessment Procedures

The Proposed Regulation provides for two different types of conformity assessments, depending on the type of high-risk AI system at issue:

1. *Internal Assessment*. This assessment does not require the involvement of an independent third party. A provider must (1) verify that the AI system's "quality management system" is in compliance with the requirements of Article 17 of the Proposed Regulation, which requires that providers implement a quality management system that incorporates many features, including risk management, post-market monitoring, procedures for reporting incidents (*e.g.*, data breaches, system malfunctioning, and identification of risks that were not previously apparent), and testing and validation procedures for data management; (2) examine the information in the AI system's technical documentation to assess the compliance of the AI system with the "relevant essential requirements" for high-risk AI systems under the Proposed Regulation; and (3) verify that the design and development process of the AI system and its post-market monitoring as set out in Article 61 of the Proposed Regulation is consistent with the system's technical documentation (this documentation includes information on the AI system's capabilities and limitations, algorithms, data, training, testing, and validation processes used).
2. *Notified Body Assessment*. This assessment is conducted by an independent third party[1] who will issue a certificate to confirm the AI system's compliance. The AI system provider will be required to submit documentation and information relating to the system's quality management system and technical documentation, which the notified body will use to determine whether the AI system meets the relevant requirements. In addition, the Proposed Regulation will require a provider to allow the notified

> body to access the premises where the design, development, and testing of the AI systems is taking place; carry out "periodic audits" to ensure the provider maintains and applies the quality management system; and, where reasonably necessary to assess conformity, access to the source code of the AI system. This requirement is similar to audits required for EU General Data Protection Regulation ("GDPR") data processing agreements where it is now common practice for processors to limit access to premises and systems and impose confidentiality restrictions. Given that a notified body is an appointed certifying entity, it is not clear whether the market will evolve to imposing similar restrictions in the context of AI conformity assessments or whether such restrictions will be permissible under the Proposed Regulation. Providers may want to consider advocating for clearer controls and confidentiality given the highly proprietary and sensitive nature of source code and algorithms of their AI systems.

While the Proposed Regulation allows for a presumption of conformity for certain data quality requirements (where high-risk AI systems have been trained and tested on data concerning the specific settings within which they are intended to be used) and cybersecurity requirements (where the system has been certified or a statement of conformity issued under a cybersecurity scheme),[2] providers are not absolved of their obligation to carry out a conformity assessment for the remainder of the requirements.

Determining Which Type of Assessment Applies

The specific conformity assessment to be conducted for high-risk AI systems depends on the category and type of AI at issue:

- For high-risk AI systems that relate to the *biometric identification and categorization of natural persons* the Proposed Regulation provides two options:
  - If harmonized standards or common specifications have been applied,[3] the provider may choose to conduct either (1) an Internal Assessment; or (2) a Notified Body Assessment.

- If harmonized standards have been only partially applied, do not exist, or common specifications are not available, the provider must conduct a Notified Body Assessment.

- For the remaining high-risk AI systems identified in the Proposed Regulation, including those that relate to the *management and operation of critical infrastructure, education and vocational training, employment, workers management and access to self-employment, or the access to and enjoyment of essential private services and public services and benefits*,[4] the Proposed Regulation allows the provider to follow the Internal Assessment procedure.

High-risk AI systems must undergo new assessments whenever they are "substantially modified," regardless of whether the modified system will continue to be used by the current user or is intended to be more widely distributed. In any event, a new assessment is required every five years for AI systems required to conduct Notified Body Assessments.

Potential Impacts

Many questions remain about how the conduct of conformity assessments will function in practice, including how the requirement will work in conjunction with UK and EU anti-discrimination legislation (*i.e.*, the UK Equality Act 2010) and existing sectoral safety legislation, as in the following subsections.

Supply Chain Impact and Division of Liability

The burdens of performing a conformity assessment will be shared among stakeholders. Prior to placing a high-risk AI system on the market, importers and distributors of such systems will be required to ensure that the correct conformity assessment was conducted by the provider of the system. Parties in the AI ecosystem may try to contract around liability issues and place the burden on parties elsewhere in the supply chain to meet conformity assessment requirements.

Costs of Compliance (and Noncompliance)

While the Proposed Regulation declares that the intent of the "conformity assessment approach [is] to minimize the burden for economic operators [*i.e.*, stakeholders]," some commentators have expressed concern that an unintended consequence will be to force providers to conduct duplicative assessments where they are already subject to existing EU product legislation and other legal frameworks.[5] Conducting a conformity assessment may also result in increased business and operational costs to businesses, such as legal fees. Companies will want to educate the EU Parliament and Council about these impacts during the legislative process through lobbying and informally, for example, during conferences typically attended by industry and regulators, and in thought leadership.

In addition to the cost of conducting a conformity assessment, penalties for noncompliance will be hefty—the Proposed Regulation tasks EU Member States with enforcement and imposes a three-tier fine regime similar to the GDPR: the higher of up to two percent of annual worldwide turnover or €10 million for incorrect, incomplete, or misleading information to notified supervisory or other public authorities; up to four percent of annual global turnover or €20 million for noncompliant AI systems; or up to six percent of annual global turnover or €30 million for violations of the prohibitions on unacceptable AI systems and governance obligations.

Extraterritorial Reach

Like the GDPR, the Proposed Regulation is intended to have global reach and applies to: (i) providers that offer AI in the European Economic Area ("EEA"), regardless of whether the provider is located in or outside the EEA; (ii) users of AI in the EEA; and (iii) providers and users of AI where the providers or users are located outside of the EEA but the AI outputs are used in the EEA. Prong (iii) could raise potential compliance headaches for providers of high-risk AI systems located outside of the EEA, who may not always be aware of or able to determine where the outputs of their AI systems are used. This may also cause providers located outside of the EEA to conduct a cost-benefit analysis before introducing their product to market in the EEA, though such providers

will likely already be familiar with conformity assessments under existing EU law.

Data Use

In conducting the conformity assessment providers will need to address data privacy considerations involving the personal data used to create, train, validate, and test AI models, including the GDPR's restrictions on automated decision-making, through corresponding data subject rights. As noted, this focus does not appear to be contemplated by existing product legislation, the focus of which was the integrity of physical products introduced into the EU market.

For AI conformity assessments, data sets must meet certain quality criteria. For example, the data sets must be "relevant, representative and inclusive, free of errors and complete." The "characteristics or elements" that are specific to the "geographical, behavioral, or functional setting" in which the AI system is intended to operate should be considered. As noted, providers of high-risk AI systems should identify the risk of inherent bias in the data sets and outputs. The use of race, ethnicity, trade union membership, and similar demographic characteristics (or proxies) (including the use of data of only one of these groups) could result in legal, ethical, and brand harm. AI fairness in credit scoring, targeted advertising, recruitment, benefits qualifications, and criminal sentencing is currently being examined by regulators in the United States and other countries, as well as by industry trade groups, individual companies, nonprofit think tanks, and academic researchers. Market trends and practices are currently nascent and evolving.

Bolstering of Producer Defenses Under the EU Product Liability Regime

Many see the European Union as the next frontier for mass consumer claims. The European Union has finally taken steps via EU Directive 2020/1828 on Representative Action ("Directive") to enhance and standardize collective redress procedures throughout the Member States. The provisions of that Directive must be implemented no later than mid-2023. Class action activity in the

European Union was already showing a substantial increase and the Directive will only enhance that development. The EU Product Liability framework is often said to be strict liability—reflecting Directive 85/374/EEC—however, importantly, under certain limited exceptions, producers can escape liability, including by asserting a "state-of-the-art" defense (*i.e.*, the state of scientific or technical knowledge at the time the product was put into circulation could not detect the defect). At least as far as this applies to an AI component, the new requirements on conformity assessments detailed above, particularly those undertaken by a notified body, may provide producers with a stronger evidential basis for asserting that defense.

Practical Tips and Takeaways

While the Proposed Regulation is currently being addressed in the tripartite process, we anticipate that its core requirements will be implemented. In order to future proof the development and use of this valuable technology, companies will want to consider the following measures to prepare:

- Providers will want to assess which conformity regime may apply to their current AI system or systems in development, including whether the system can rely on a presumption of conformity.
- Consider incorporating the conformity assessment requirements into the AI product development process, instead of at or after launch to mitigate risk of enforcement and remedies that, in addition to monetary fines, could include deletion of the AI system and underlying data.
- Consider legal feasibility of ongoing testing once the product has been introduced into the market.
- Importers and distributors of AI systems will want to review contracts with providers and update them to bind providers to comply with conformity assessment obligations.
- Consider whether data subject GDPR rights can be addressed, given the nature of AI systems, and whether there are technical means (*e.g.*, anonymization), to overcome corresponding obligations.

- Monitor parallel AI legislation or initiatives, such as the recently released UK AI Strategy and U.S. regulator enforcement actions and policy statements, that could create a patchwork of conflicting or burdensome obligations.

Remember the new obligations may be your friend. Class actions are on the rise in the EU Member States and the Directive must be implemented in all Member States by 2023. Careful record keeping on testing and decision making about product launches may assist a producer's defense if it becomes a target.

Notes

* Karen L. Neuman, a partner at Dechert LLP and global co-chair of its privacy and cybersecurity practice, was the former chief privacy officer for the U.S. Department of Homeland Security. Dorothy Cory-Wright is a partner at the firm, advising on complex commercial litigation, arbitration, alternative dispute resolution, and contentious regulatory issues, including monitorships. Colleen B. Hespeler is an associate in the firm's privacy and cybersecurity practice group. Madeleine White is an associate at the firm and member of the intellectual property and privacy and cybersecurity practices. The authors may be reached at karen.neuman@dechert.com, dorothy.cory-wright@dechert.com, colleenb.hespeler@dechert.com, and madeleine.white@dechert.com, respectively.

1. The Proposed Regulation provides for the establishment of "notified bodies" within an EU member state. Notified bodies will be required to perform the third-party conformity assessment activities, including testing, certification, and inspection of AI systems. In order to become a notified body, an organization must submit an application for notification to the notifying authority of the EU member state in which they are established.

2. Pursuant to Regulation (EU) 2019/881.

3. "Harmonised standard" is defined in the Proposed Regulation as a European standard as defined in Article 2(1)(c) of Regulation (EU) No. 1025/2012. "Common specifications" is defined as a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under the Proposed Regulation.

4. The other high-risk AI systems identified in the Proposed Regulation relate to law enforcement, migration, asylum and border control management, and administration of justice and democratic processes.

5. For example, MedTech Europe submitted a response to the Proposed Regulation, arguing that it would require manufacturers to "undertake

duplicative certification/conformity assessment, via two Notified Bodies, and maintain two sets of technical documentation, should misalignments between [the Proposed Regulation] and MDR/IVDR not be resolved." Available at https://www.medtecheurope.org/wp-content/uploads/2021/08/medtech-europe-response-to-the-open-public-consultation-on-the-proposal-for-an-artificial-intelligence-act-6-august-2021-1.pdf.