EU AI Act: Enforcement insights and guidance for businesses

Lorraine Maisnier-Boché, **Pilar Arzuaga** and **Simon Mortier** of McDermott Will & Emery
report on the EU AI Act which is expected to enter into force in May.

The EU AI Act introduces a groundbreaking framework for regulating artificial intelligence (AI) across Europe, categorizing AI systems into four risk levels: Prohibited AI, High-Risk AI, Limited Risk AI, and Minimal Risk AI. Each category demands specific compliance measures, impacting a wide array of sectors such as healthcare, finance, and consumer technologies. The Act's broad scope introduces complexity to its enforcement, handled primarily by national market surveillance authorities within Member States and supported by the newly established AI Office at the EU level for overseeing general-purpose AI models.

The newly established AI Office is competent for general-purpose AI models. However, there are cases where competences may overlap, and EU Member States have the discretion to designate one or several competent authorities.

The AI Act, expected to come into effect in May 2024, mandates Member States to appoint their market surveillance authorities within 12 months. Businesses are urged to engage with relevant authorities to ensure compliance and mitigate risks. Participation in the "AI Pact", a voluntary initiative by the EU Commission, is recommended for businesses to anticipate compliance requirements and showcase leadership in ethical AI governance.

This article aims to clarify the AI Act's enforcement mechanisms, detailing the roles of authorities at Member State and EU levels, and guiding businesses through the regulatory landscape. It highlights the necessity for businesses to understand their obligations under the Act and to prepare for compliance.

Member State level

National market surveillance authorities, competent for AI systems: The AI Act builds upon the existing EU general framework for market surveillance of manufactured products (excluding food, feed, medicinal products, plants and animals, products of human origin that are subject to specific market surveillance regulations), under Regulation (EU) 2019/1020[1].

Each EU Member State must appoint at least one national market surveillance authority, responsible for overseeing the application and implementation of the AI Act, in addition to conducting market surveillance activities for almost all AI systems. Moreover, in order to improve organisational effectiveness across Member States, each one is required to designate a market surveillance authority as single point of contact for the public and for coordination with counterparts at Member State and Union levels.

Determining which existing national authority will assume the role of market surveillance authority is crucial. It is probable that multiple authorities could be designated per Member State, especially when AI systems are specific to a sector already under the supervision of a regulatory authority (such as medical devices). For EU institutions, the AI Act has already designated the European Data Protection Supervisor (EDPS) as the competent authority.

Like any market surveillance authority under Regulation (EU) 2019/1020, national authorities will have the power to request corrective measures and impose administrative fines. Fines for non-compliance with AI regulations are tiered, reaching up to 7% of global annual turnover or €35 million for prohibited AI violations, up to 3% or €15 million for other infringements, and up to 1.5% or €7.5 million for providing incorrect information - whichever is higher, except for SMEs and start-ups, where the rule of whichever is lower applies. The European Commission will issue guidelines to help Member States align their national rules and practices.

Notifying authorities competent for AI conformity assessment bodies: Given the complexity of high-risk AI systems and their associated risks, the AI Act establishes a system of conformity assessments for systems that involve third-party conformity assessment bodies (also known as "notified bodies"). These bodies carry out third-party conformity assessment activities, including testing, certification, and inspection.

Member States are required to designate notifying authorities responsible for setting up and implementing procedures for the assessment, designation, and notification of these conformity assessment bodies, as well as monitoring them. These procedures are to be developed in collaboration with the notifying authorities across the Member States. Additionally, Member States have the option to delegate the assessment and monitoring roles to a national accreditation body, in accordance with Regulation (EU) 765/2008[2].

The notifying authorities must organise their operational framework to ensure no conflicts of interest with conformity assessment bodies, maintaining objectivity and impartiality of their activities. Individuals who decide on the notification of conformity assessment bodies should not be involved in evaluating these bodies.

Furthermore, notifying authorities are prohibited from engaging in the provision of activities or consultancy services similar to those rendered by conformity assessment bodies, on a commercial or competitive basis. They are also required to guarantee the confidentiality of information and to staff their operations with individuals who possess the necessary competence, including expertise in information technologies, artificial intelligence, legal standards, and the oversight of fundamental rights.

EU LEVEL

AI Office, centre of AI expertise for general-purpose AI models: Established on 24 January 2024[3], before the AI Act's adoption, the AI Office within the European Commission is set to play a key role in shaping AI policy at EU level. Its wide-ranging mandate includes coordinating EU stakeholders, aiding market surveillance authorities across Member States, and developing AI-related tools, methodologies, guidance, and codes of practice. More specifically, the AI Office is also tasked with enhancing EU expertise and capabilities in the field of AI and to serve as a bridge to the scientific community.

The AI Office will also hold a more specific responsibility for overseeing the enforcement of rules related to general-purpose AI models. While national market surveillance authorities are responsible for the supervision of AI systems, the AI Office is primarily in charge of general-purpose AI models. It will have the authority to request information and documentation, evaluate these models, and investigate potential rule violations, including gathering complaints and alerts.

A scientific panel of independent experts will assist the AI Office's monitoring activities by providing alerts when a general-purpose AI model is suspected of posing a concrete and identifiable risk at Union level, or if it potentially meets the criteria for a model with systemic risk. These alerts are designed to trigger further investigative actions.

Should the evaluation process reveal serious and substantiated systemic risk concerns at the EU level, the European Commission has the power to require providers to implement mitigation measures. These measures may include limiting the market availability of the implicated AI model through withdrawal or recall. Additionally, the European Commission can impose fines on providers of general-purpose AI models that do not exceed 3% of their total worldwide turnover in the preceding financial year or EUR 15 million, whichever is higher.

AI Board, an advisory body: An 'AI Board' will be established, composed of national authorities selected by each Member State to represent their interests on the AI Board, in addition to the EDPS, and the European Commission. Similar to the role played by the European Data Protection Board (EDPB) in the enforcement of the General Data Protection Regulation (EU) 2016/679 (GDPR), the AI Board will also serve an advisory and harmonization function. It will provide guidance on the Act's uniform implementation, issue recommendations and opinions — particularly concerning high-risk AI systems — facilitate coordination between national authorities, and promote standardization efforts.

THE INTERPLAY BETWEEN COMPETENT EU AND NATIONAL AUTHORITIES

To prevent overlapping competences and ensure the coordinated regulation of general-purpose AI models and their associated systems, the AI Act encourages instances of cooperation and even the exchange of competences between national market surveillance authorities and the AI Office.

For example, market surveillance authorities must cooperate with the AI Office to carry out evaluations of compliance, where a general-purpose AI system is directly used by deployers for at least one purpose considered high-risk. Similarly, market surveillance authorities may seek assistance from the EU AI Office if they are unable to complete an investigation on a high-risk AI system due to lack of access to certain information about the general-purpose AI model on which the high-risk AI system is built.

In cases where an AI system employs a general-purpose AI model from the same provider, the AI Office takes on oversight responsibilities and assumes enforcement capabilities typical of a market surveillance authority.

CONCLUSIONS AND NEXT STEPS FOR BUSINESSES

Identifying the competent EU or national authority for enforcing and overseeing the AI Act is crucial for ensuring regulatory compliance, obtaining guidance, managing risks, and promoting innovation. Engaging with the relevant authority and adhering with its guidelines can help prevent legal and financial consequences, earn user trust, and unlock new market opportunities.

To accurately identify the relevant authority, businesses should conduct a thorough assessment of their AI systems and models. This evaluation should categorise the systems and models based on their characteristics, risk level, application area, and geographical deployment.

Additionally, businesses should be aware of the 'AI Pact', initiated by the European Commission. This initiative encourages organisations to prepare for the AI Act by voluntarily sharing their internal guidelines, processes and the specific actions they have undertaken to meet the requirements of the AI Act, as well as by testing their solutions within the community. Participating in such voluntary commitments to comply with the AI Act's requirements before the deadlines can position organisations as leaders in ethical AI usage and governance and enhance their future interactions and relationship with EU or national authorities.

AUTHORS

Lorraine Maisnier-Boché, Counsel (Paris), Pilar Arzuaga, Senior Associate (London), Simon Mortier, Senior Associate (Brussels), McDermott Will & Emery.
Emails: lmaisnierboche@mwe.com, parzuaga@mwe.com, smortier@mwe.com

REFERENCES

1 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, as amended.
2 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, as amended.
3 Decision of the EU Commission of 24 January 2024 establishing the European Artificial Intelligence Office.

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

CJEU rules on SCHUFA's automated decision-making

A broad interpretation of 'automated decision-making' means that a range of automated processes may be caught for both credit scoring and other contexts, such as recruitment. By **Katharina A. Weimer** of Fieldfisher Germany.

In its long-awaited decision in proceedings between an individual and the Federal State of Hessen, Germany, (Hessen) (C-634/21)[1] the Court of Justice of the European Union (CJEU) has now interpreted the "automated decision-making" framework under the GDPR. The CJEU ruled in its judgment on 12 January 2024 that a credit scoring

Continued on p.3

Israel's EU adequacy status renewed – a surprise and a relief

Professor Michael Birnhack of Tel Aviv University analyses the EU's recent positive adequacy decision on Israel.

The EU's decision to reaffirm Israel's adequacy status was received by the local privacy community with relief, and with some surprise. The relief is due to the importance of the decision for the local economy, and the negative economic and political implications that would have occurred, had an adverse decision been reached. The moderate surprise is due to the persistent gaps between Israeli data protection law and the GDPR which are quite substantial.

Continued on p.5

Issue 188 **APRIL 2024**

COMMENT

NEWS

ANALYSIS

LEGISLATION

MANAGEMENT

NEWS IN BRIEF

INTERNATIONAL
report

ISSUE NO 188 APRIL 2024

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
g.greenleaf@iinet.net.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Katharina A. Weimer
Fieldfisher, Germany
Professor Michael Birnhack
Tel Aviv University, Israel
Nana Botchorichvili
IDEA Avocats, France
Poojan Bulani
University College London, UK
Yan Luo and Xuezi Dan
Covington, US and China
Merrill Dresner
PL&B Correspondent
Affiliated Associate Professor Elizabeth Coombs
University of Malta, Malta
Associate Professor Elif Küzeci
Bahçeşehir University, Türkiye
Lorraine Maisnier-Boché, Pilar Arzuaga and Simon Mortier
McDermott Will & Emery, France, UK and Belgium

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Balancing privacy with data-crunching AI

The EU AI Act will soon be reality (p.29), and we watch with interest which regulators will be given the task to enforce the Act at national level. The EU AI Office will coordinate enforcement action across the EU on prohibited and high-risk AI systems (p.30). Will it function in a similar fashion to the European Data Protection Board (EDPB) in its efforts to ensure consistency in Member States? Its AI Board with Member States' representatives may conduct joint investigations, but will not have direct enforcement powers.

Meanwhile, the EU Commission is evaluating how the GDPR is working in practice. Results are expected by this summer (p.7). A topic that has gained much attention is legal bases for behavioural advertising and the so-called Pay or Consent model. The EU DPAs are soon to issue an opinion on this subject (p.26). Italy's Data Protection Authority, the *Garante*, is actively enforcing the GDPR in relation to OpenAI, the company behind ChatGPT's AI platform. Also, the EDPB has a taskforce on this issue. Both of these topics will be discussed in detail at our Annual Conference in July, with Meta, the EU Commission, the *Garante*, EDPB and OpenAI speaking – see www.privacylaws.com/plb2024

AI-aided surveillance will be in action at the Paris 2024 summer Olympic Games (p.11). Our second article from France looks at the CNIL's €32 million fine on Amazon Logistique for its employee data processing (p.8). In this issue, we also bring you AI developments from the Asia-Pacific region (p.13), our first in-depth analysis of 20 Caribbean privacy laws (p.18), stronger regulatory powers in Ontario, Canada (p.15) and new international transfer rules in Türkiye (p.28). Read on p.1 an analysis of Israel's renewed EU adequacy decision, and the implications of a CJEU ruling on automated decision-making by a credit scoring agency.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.