ARTICLE | August 6, 2024

EU AI Act: Obligations for Deployers of High-Risk AI Systems

What companies need to know to comply with the complex landscape of new obligations.

Now that the EU AI Act has come into force, companies deploying high-risk artificial intelligence (AI) systems in the European Union (EU) must prepare to navigate a complex landscape of new obligations by 2 August 2027. This article explains these obligations so that companies can implement them strategically.

Classification

In practical terms, a "deployer" is any legal entity using an AI system in a professional capacity under its authority. Deployers are subject to the AI Act if they are established or located in the EU or if the output of the AI system is used in the EU. High-risk AI systems are those that pose a significant risk to health, safety, or fundamental rights and are specifically defined as high risk in the AI Act, including AI systems used for:

- selecting, monitoring, or evaluating employees;
- credit checks / credit scores; or
- profiling individuals in certain situations (e.g., in a credit-rating context).

Each system must be individually assessed to determine if it falls under this category.

Key Obligations

1. Training and Support Obligations

   - **AI literacy training:** Ensure all users have sufficient AI knowledge and information to use the AI system as intended.
   - **Training and support of overseers:** Provide necessary training and support for those overseeing the respective high-risk AI system to ensure that they have the necessary competence and authority to carry out that role. Specifically, ensure that overseers receive guidance on when and how to make informed decisions in order to avoid negative consequences or risks, or stop the high-

risk AI system if it is not performing as intended.

2. Operational Obligations

   - **Technical and organizational measures:** Implement appropriate technical and organizational measures to ensure that use of the high-risk AI systems is in accordance with the instructions of use.
   - **Input data quality management:** Ensure input data is representative, qualitative, and relevant for the AI system's intended purpose.
   - **Suspension of operation:** Suspend use if the high-risk AI system poses a risk or does not perform as intended.

3. Control and Risk-Management Obligations

   - **Pre-check for prohibited practices:** Ensure the AI system does not engage in any of the prohibited practices defined in the AI Act.
   - **Impact assessment:** Where applicable, carry out, document, and maintain a fundamental rights impact assessment in relation to the AI system, and inform the national authority of the results of the assessment.
   - **Human oversight:** Assign competent individuals to oversee the functioning of the AI system and implement the human oversight measures indicated by the providers.
   - **Continuous monitoring:** Regularly monitor the AI system for risks, including in view of detecting and addressing anomalies, dysfunctions, and unexpected performance.

4. Documentation Obligations

   - **Recordkeeping:** Maintain logs of the high-risk AI system's operations for at least six months.
   - **Other legal acts:** Establish documentation required under other legal acts (e.g., GDPR accountability documentation, including DPIA as the case may be).

5. Notification and Transparency Obligations

   - **Providers:** Inform provider of this high-risk AI system of any relevant operational circumstances occurring, as per the instructions to be supplied by the provider.
   - **Risks or incidents:** Notify providers and authorities in case of risks to the health, safety, or fundamental rights of individuals or a serious incident.
   - **Employees and individuals:** Inform individuals that may be affected by results derived from high-

risk AI system about the use of this AI system.

6. Compliance Obligations With Other Legal Acts

   - Ensure all AI-related data processing complies with other EU and national laws, in particular with the GDPR, national laws under the ePrivacy Directive (on the use of cookies and digital marketing), the EU Data Act, and relevant cybersecurity laws.

7. Cooperation Obligations

   - **EU and national authorities:** Cooperate with EU and national authorities and engage in voluntary codes of practice and guidance.

8. Additional Provider Obligations

   - **White labeling or modifications:** Determine if the AI system is deployed on a white-labeled basis (i.e., the AI system is provided by a third party but labeled with the deployer's firm name or branding) or has been substantially modified or is used for modified high-risk purposes. In these circumstances, the deployer may be subject to the considerable additional obligations applicable to providers of high-risk AI systems under the AI Act.

Recommendations

Companies deploying high-risk AI systems in the EU should begin integrating the AI Act requirements into their planning now. Companies should use existing processes, such as those for GDPR compliance, to meet new obligations. Finally, companies should engage with their AI system providers and anticipate

Checklist: Obligations for Deployers of High-Risk AI Systems

Training and Support Obligations

- AI literacy training
- Training and support of overseers

Operational Obligations

- Technical and organizational measures to ensure use in accordance with the instructions
- Input data quality management
- Suspension of operation if risk present

Control and Risk-Management Obligations

- Pre-check for prohibited practices, Art. 5 AI Act
- Fundamental rights impact assessment
- Human oversight
- Continuous monitoring

Documentation Obligations

- Recordkeeping

Notification and Transparency Obligations

- Toward providers in relevant operational circumstances
- Toward providers and authorities in case of serious incidents
- Toward employees and individuals

Compliance Obligations With Other Legal Acts

- In particular, GDPR compliance

Cooperation Obligations

- With EU and national authorities

Additional Provider Obligations

- White-labeled or modified high-risk AI systems

Contacts:

Gail E. Crawford
London
gail.crawford@lw.com
+44.20.7710.3001

Jean-Luc Juhan
Paris
jean-luc.juhan@lw.com
+33.1.4062.2000

Hanno F. Kaiser
San Diego / San Francisco
hanno.kaiser@lw.com
+1.858.509.8458

Susan Kempe-Mueller
Frankfurt
susan.kempe-mueller@lw.com
+49.69.6062.6580

Deborah J. Kirk
London
deborah.kirk@lw.com
+44.20.7710.1000

Fiona M. Maclean
London
fiona.maclean@lw.com
+44.20.7710.1822

Elisabetta Righini
Brussels
elisabetta.righini@lw.com
+32.2.788.6238

Michael H. Rubin
San Francisco
michael.rubin@lw.com
+1.415.395.8154

Myria Saarinen
Paris
myria.saarinen@lw.com
+33.1.4062.2000

Tim Wybitul
Frankfurt
tim.wybitul@lw.com
+49.69.6062.6560