Checklist

Assessing EU AI Act Risks

Contributed by Michael Kearney and Tara Emory, Redgrave Data

Bloomberg Law

Assessing EU Artificial Intelligence (AI) Act Risks

*Contributed by **Michael Kearney** and **Tara Emory**, Redgrave Data*

Companies seeking to ensure that they meet the requirements of the European Union's (EU) Artificial Intelligence Act (**AI Act**) should first conduct a thorough audit to determine their compliance obligations under the law. This audit should include the following elements:

- ☐ **Take inventory of systems, stakeholders, and applications.**
  - ☐ Determine use of AI systems by each organizational function/department.
  - ☐ Review IT processes and documentation for organizational use of AI, including processes for approving AI application use.
  - ☐ Review existing applications to check for newly incorporated AI capabilities available to employees and not previously documented.
  - ☐ Review any existing AI policies and other or related policies such as device usage.
  - ☐ Identify AI Governance/Ethics Team and inclusion of appropriate stakeholder participation; consider initiating a team if it does not exist.

- ☐ **For each AI use in the organization, evaluate the applicability of EU AI Act (and other AI regulations).**
  - ☐ Check whether the use is covered by the EU AI Act definitions.
  - ☐ Determine whether your organization acts as a provider, deployer, distributor, or importer of the AI system.
  - ☐ Determine whether you are a provider of any general purpose Large Language Models (**LLMs**).
  - ☐ Confirm that AI system application is not prohibited, such as subliminal techniques, manipulating vulnerable individuals, social scoring, and certain uses of biometric data.
  - ☐ Determine risk level of AI System (high-risk, limited risk, or minimal/none)
    - Complete conformity assessment for high-risk.
    - Determine any need for end-user transparency.
  - ☐ Assess General Data Protection Regulation (**GDPR**) compliance for any private data involved in AI system.
  - ☐ Assess compliance with any applicable EU product governance.
  - ☐ Check for other applicable regulations (e.g., **US state laws**).
  - ☐ Assess any material updates to AI system.
  - ☐ Incorporate recommended practices from standard-setting groups, which can create a presumption of conformity. Consider:
    - European Committee for Standardization (**CEN**);
    - European Committee for Electrotechnical Standardization (**CENELEC**);
    - International Organization for Standardization (**ISO**); and
    - International Electrotechnical Commission (**IEC**).

- ☐ **Think about current governance practices and requirements, including:**
  - ☐ Records retention and management;
  - ☐ Privacy requirements;
  - ☐ Reasonable security;
  - ☐ Planning and design;
  - ☐ Inputs;
  - ☐ Model applied;
  - ☐ Context;
  - ☐ Updates; and
  - ☐ End of life

- ☐ **Determine how to incorporate EU AI Act requirements into existing current** governance practices, including considerations of the following:
  - ☐ Overall risk management system;
  - ☐ Data and data governance;
  - ☐ Technical documentation;
  - ☐ Record-keeping;
  - ☐ Transparency and the provision of information to deployers;
  - ☐ Human oversight;
  - ☐ Accuracy, robustness, and cybersecurity;
  - ☐ Role-specific obligations;
    - Providers
    - Importers
    - Distributors
    - Deployers
    - Manufacturers
    - Authorized Representatives
  - ☐ Specific conformity assessment; and
  - ☐ Updates to applicable policies.

- ☐ **Determine whether you should consult other parties and sources, including:**
  - ☐ Whether third-parties are needed for conformity assessments or if you can rely on existing internal controls;
  - ☐ Other emerging best practices (e.g., **NIST**); and
  - ☐ Updated EU guidance.