Volume 2, Number 1 January–February 2025

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

Editor's Note: Obligations
Victoria Prussen Spears

How the Corporate Sustainability Due Diligence Directive Will Change ESG Obligations for Companies Operating in the EU—A Comparison of Existing French and German Due Diligence Legislations
Thomas Delille, Sepp Wohlfarter, Marion Seranne, and Nora Thies

Obligations for Deployers, Providers, Importers, and Distributors of High-Risk AI Systems in the European Union's Artificial Intelligence Act
Martin Braun, Anne Vallery, and Itsiq Benizri

Court Overturns European Commission's Approach to "Killer Acquisitions"
Laurence Bary, Michael I. Okkonen, Mélanie Thill-Tayara, Clemens Graf York von Wartenburg, Marion Provost, Alec Burnside, and Lucas Leroy

Consent or Pay in the European Union: One Rule for Some (Large Online Platforms), Another Rule for Everyone Else?
Barry Fishley and Chloe Kite

Upcoming European Union Regulation Concerns Forced Labour in Supply Chains
Aline Doussin, Lourdes Catrain, Daniel Shapland, Pierre Estrabaud, and Helka Kittila

Renewable Energy Outlook for Asia and the Middle East
James Clark and Aurelia Russo

Mexico's Energy Regulatory Commission Publishes on Electromobility in Mexico
Rodolfo Rueda, Gerardo Prado Hernandez, Adrián Ortiz de Elguea, and Mariana Salinas

Fiduciary Liens Over Immovable Property in Brazil: Advancements and Setbacks
Paulo Fernando Campana Filho

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 2, No. 1 January–February 2025

5 **Editor's Note: Obligations**
Victoria Prussen Spears

9 **How the Corporate Sustainability Due Diligence Directive Will Change ESG Obligations for Companies Operating in the EU—A Comparison of Existing French and German Due Diligence Legislations**
Thomas Delille, Sepp Wohlfarter, Marion Seranne, and Nora Thies

23 **Obligations for Deployers, Providers, Importers, and Distributors of High-Risk AI Systems in the European Union's Artificial Intelligence Act**
Martin Braun, Anne Vallery, and Itsiq Benizri

37 **Court Overturns European Commission's Approach to "Killer Acquisitions"**
Laurence Bary, Michael I. Okkonen, Mélanie Thill-Tayara, Clemens Graf York von Wartenburg, Marion Provost, Alec Burnside, and Lucas Leroy

49 **Consent or Pay in the European Union: One Rule for Some (Large Online Platforms), Another Rule for Everyone Else?**
Barry Fishley and Chloe Kite

55 **Upcoming European Union Regulation Concerns Forced Labour in Supply Chains**
Aline Doussin, Lourdes Catrain, Daniel Shapland, Pierre Estrabaud, and Helka Kittila

59 **Renewable Energy Outlook for Asia and the Middle East**
James Clark and Aurelia Russo

67 **Mexico's Energy Regulatory Commission Publishes on Electromobility in Mexico**
Rodolfo Rueda, Gerardo Prado Hernandez, Adrián Ortiz de Elguea, and Mariana Salinas

71 **Fiduciary Liens Over Immovable Property in Brazil: Advancements and Setbacks**
Paulo Fernando Campana Filho

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL (ISSN 2995-7486) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Leanne Battle
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

The photo on this journal's cover is by Gaël Gaborel—A Picture of the Earth on a Wall—on Unsplash

Cite this publication as:

The Global Regulatory Developments Journal (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and others interested in global regulatory developments.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Leanne Battle, Publisher, Full Court Press at leanne.battle@vlex.com or at 866.773.2782

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2995-7486

Obligations for Deployers, Providers, Importers, and Distributors of High-Risk AI Systems in the European Union's Artificial Intelligence Act

Martin Braun, Anne Vallery, and Itsiq Benizri*

In this article, the authors focus on obligations that the EU's Artificial Intelligence Act sets for deployers, providers, importers, and distributors regarding high-risk AI systems.

The EU's Artificial Intelligence Act's (AI Act) overall risk-based approach means that, depending on the level of risk, different requirements apply.[1] In total, there are four levels of risk:

1. Unacceptable risk, in which case AI systems are prohibited;
2. High risk, in which case AI systems are subject to extensive requirements, including regarding transparency;
3. Limited risk, which triggers only transparency requirements; and
4. Minimal risk, which does not trigger any obligations.

Key Players

The AI Act identifies and defines the following key players, all of which can be natural or legal persons:

- *Deployers* use AI under their authority in the course of their professional activities. In practice, it is likely that companies will quickly be above this very low threshold.
- *Providers* develop AI systems with a view to placing them on the market or putting them into service under their own name or trademark, whether for payment or free of charge.

The Global Regulatory Developments Journal / January–February 2025, Vol. 2, No. 1, pp. 23–35.

ISSN 2995-7486.

- *Importers* are located outside the European Union and place on the market AI systems bearing the name or trademark of a natural or legal person established outside the European Union.
- *Distributors* are players in the supply chain, other than the provider or the importer, that make an AI system available on the EU market.

Obligations for Deployers of High-Risk AI Systems

- *Instructions for Use*. Deployers must take appropriate technical and organizational measures to ensure they use high-risk AI systems in accordance with the instructions for use. EU or national law can impose additional obligations in this respect.
  - *Monitoring*. Deployers must monitor the operation of the system on the basis of the instructions for use. Where relevant, deployers must inform providers.
  - *Risk to Health, Safety, or Fundamental Rights*. Where deployers have reasons to believe that using the system in accordance with the instructions may adversely affect individuals' health, safety, or fundamental rights (see above), they must, without undue delay, inform the provider or distributor and the relevant market surveillance authority. They should also suspend the use of the system.
  - *Serious Incident*. Where deployers have identified a serious incident, they must immediately inform first the provider and then the importer or distributor and the relevant market surveillance authorities. If the deployer is unable to contact the provider, it must inform the market surveillance authority of the European country where the incident occurred. This should occur immediately after establishing a causal link between the AI system and the serious incident, or the reasonable likelihood of such a link. In any case, this notification should take place no later than 15 days after the deployer becomes aware of the incident.

    - *Logs*. Deployers of high-risk AI systems must retain the logs automatically generated by the system, to the extent that such logs are within their control, for a duration appropriate to the system's intended purpose but of at least six months, unless provided otherwise in applicable EU or national law.
    - *Input Data*. If the deployer exercises control over the input data, it must ensure that such data is relevant and sufficiently representative in view of the intended purpose of the system.
- *Human Oversight*. Deployers must assign human oversight to individuals who have the necessary competence, training, authority, and support. Deployers are free to organize their own resources and activities to implement the oversight measures indicated by the provider. EU or national law can impose additional obligations. The above requirement regarding input data also applies.
- *Workplace*. Before putting into service or using a high-risk AI system in the workplace, deployers that are employers must inform workers' representatives and the affected workers that they will be subject to the use of a high-risk AI system.
- *Transparency*. Deployers of specific high-risk AI systems listed in the AI Act (e.g., those used in critical infrastructures, education and vocational training, employment, worker management, and access to self-employment) that make decisions or assist in making decisions related to natural persons must inform these persons that they are subject to the use of the high-risk AI system.
- *Cooperation with Authorities*. Deployers must cooperate with the relevant national competent authorities in any action those authorities take in relation to the high-risk AI system to implement the AI Act.
- *Fundamental Rights Impact Assessment*. Before deploying high-risk AI systems to evaluate individuals' creditworthiness, establish their credit score (excluding systems used to detect financial fraud), or assess risks and determine pricing for life and health insurance, deployers must assess the impact on fundamental rights that the use of such system may entail. This assessment must consider the processes in which the system will be employed, the duration

and frequency of its usage, the categories of individuals affected, the specific risks of harm, the measures for human oversight, and the actions to be taken if risks materialize.

- *First Use*. This obligation only applies to the first use of the high-risk AI system. The deployer may, in similar cases, rely on previous fundamental rights impact assessments or existing assessments carried out by the provider. However, the deployer needs to update such assessments as appropriate.
- *Notification to Authorities*. The deployer must inform the market surveillance authority of the results of its assessment, with only limited exemptions.
- *Data Protection Impact Assessment*. If any of the obligations in relation to the fundamental rights impact assessment is already complied with as a result of a General Data Protection Regulation data protection impact assessment, the fundamental rights impact assessment must complement that data protection impact assessment.

Obligations for Providers of High-Risk AI Systems

Providers of high-risk AI systems must ensure that their systems comply with the requirements associated with such systems and demonstrate such compliance to national competent authorities on request. Providers must also indicate on their system or, if that is not possible, on the packaging or accompanying documentation their name, registered trade name or trademark, and the address at which they can be contacted. In addition, providers must comply with the following requirements:

- *Put in Place a Quality Management System to Ensure Compliance*. This system must be documented in a systematic and orderly manner, comprising written policies, procedures, and instructions, in proportion to the size of the provider. The system must include minimum information as listed in the AI Act, such as a strategy for regulatory compliance; techniques, procedures, and systematic actions for the design control and verifications; examination, test, and

validation procedures during and after the development of the system; technical standards and specifications to ensure compliance; risk management and post-market monitoring systems; incident reporting procedures; and an accountability framework setting out individuals' responsibilities.

- *Keep the Required Documentation for 10 Years After the System Has Been Placed on the Market or Put into Service in the European Union*. This documentation must include the technical documentation and the documentation concerning the quality management system, the EU declaration of conformity and any document issued by conformity assessment bodies.
- *Keep the Logs Automatically Generated by the System to the Extent They Are Under Providers' Control*. Providers must keep the logs for a period appropriate to the intended purpose of the system but of at least six months, unless provided otherwise in relevant EU or national law.
- *Ensure That the System Undergoes the Conformity Assessment Procedure Before Being Placed on the Market or Put into Service in the European Union*. This procedure varies depending on the type of high-risk system. Providers of AI systems used for biometric purposes can choose either an internal control procedure or an external control by a conformity assessment body, provided they have applied specific technical standards. For other high-risk AI systems identified in the AI Act, providers can follow the conformity assessment procedure based on internal control. Specific rules apply to AI systems covered by EU harmonized legislation. Essentially, for some of them, the main rule is that providers must follow the procedure required under the relevant legislation.
- *Draw Up an EU Declaration of Conformity with the Requirements Associated with High-Risk AI Systems*. The provider must draw up a written, machine-readable physical or electronically signed EU declaration of conformity for each high-risk AI system and keep it at the disposal of the national competent authorities for 10 years after the system has been placed on the market or put into service. The declaration of conformity must contain the information set out in the AI Act. The European Commission may update this list in future. This information includes,

for example, information allowing the identification and traceability of the system, a statement that the declaration of conformity is issued under the sole responsibility of the provider, and references to technical standards or specifications in relation to which conformity is declared.

- *Affix the CE Marking to the System or, Where That Is Not Possible, on Its Packaging or Its Accompanying Documentation to Indicate Conformity with the AI Act*. The marking refers to the letters "CE," signifying that a product sold in the European Union has been assessed to meet the relevant protection requirements.
- *Comply with the Registration Obligations*. Before placing a high-risk AI system on the market or putting it into service (except for critical infrastructures), providers (or authorized representatives) must register themselves and their systems in the EU database.
- *Ensure Post-Market Monitoring*. Providers must establish and document a post-market monitoring system in a manner that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system. The monitoring system must actively and systematically collect, document, and analyze relevant data that may be provided by deployers or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and that allows the provider to evaluate the continuous compliance of AI systems with the AI Act. The post-market monitoring system must be based on a post-market monitoring plan, which should be part of the technical documentation drawn up before the AI system is placed on the market or put into service in the European Union. The European Commission will create a template for the monitoring plan and specify the elements that it should include.
- *Report Serious Incidents*. Providers must report any serious incident to the market surveillance authorities of the European country where that incident occurred. Serious incidents are incidents or malfunctioning of an AI system that (in)directly leads to the death of a person or serious harm to a person's health, serious and irreversible disruption of the management or operation of critical infrastructure, infringement of obligations under EU law intended to

protect fundamental rights, or serious harm to property or the environment. In specific cases, the reporting requirement is limited to the two latter cases.

The timing for reporting serious incidents varies depending on the context. Where necessary to ensure timely reporting, providers or, where applicable, deployers may submit an initial incomplete report followed by a complete one.

- *General Rule*. In general, providers must report serious incidents immediately after having established a causal link between the AI system and the incident or the reasonable likelihood of such a link. In any event, taking into account the severity of the incident, providers must make the report no later than 15 days after they or, where applicable, deployers become aware of the incident.
- *Critical Infrastructures and Widespread Infringement*. The report must be provided immediately and not later than two days after the provider or, where applicable, the deployer becomes aware of an incident or malfunctioning of an AI system that leads to a serious and irreversible disruption of the management or operation of critical infrastructure, or of a widespread infringement. A widespread infringement consists of any act or omission that is contrary to EU law protecting the interests of individuals and has harmed or is likely to harm the collective interests of individuals residing in at least two European countries other than the one in which the act or omission originated or took place, the provider (or its authorized representative) is located or established, or the deployer that committed the infringement is established. A widespread infringement may also consist of any acts or omissions contrary to EU law protecting the interests of individuals that have caused, cause, or are likely to cause harm to the collective interests of individuals and have common features, including the same unlawful practice or the same interest being infringed, and are occurring concurrently, committed by the same player, in at least three European countries.
- *Death*. In the event of the death of a person, the report shall be provided immediately after the provider or the deployer has established, or as soon as it suspects, a causal relationship between the high-risk AI system and the

serious incident but not later than 10 days after the date on which the provider or, where applicable, the deployer becomes aware of the serious incident.

- *Ensure Follow-Up on Reporting Serious Incidents*. Following the reporting of a serious incident, the provider must, without delay, perform the necessary investigation, perform a risk assessment and take corrective action. The provider must also cooperate with the competent authorities (and the conformity assessment bodies, if applicable). In this context, the provider must inform authorities before altering the AI system in a way that may affect any subsequent evaluation of the causes of the incident.
- *Take the Necessary Corrective Actions and Provide the Required Information*. If providers consider that a high-risk AI system is not in conformity with the AI Act, they must immediately take corrective actions to bring that system into conformity, withdraw it, disable it, or recall it, as appropriate. Providers must inform distributors and, where applicable, the authorized representative and importers accordingly. Providers must also immediately investigate the causes and inform market surveillance authorities (and possibly conformity assessment bodies) if they become aware of the fact that a high-risk AI system has the potential to adversely affect individuals' health, safety, or fundamental rights to a degree that goes beyond that considered reasonable and acceptable in relation to its intended purpose or under normal or reasonably foreseeable conditions of use. In particular, providers must highlight the nature of the noncompliance and of any relevant corrective action taken.
- *Ensure That the High-Risk AI System Complies with Accessibility Requirements for Certain Products and Services*. For businesses, this essentially refers to products and services identified in Directive 2019/882.[2] Examples include computers and operating systems for those computers, payment terminals, terminals used for electronic communication or audiovisual media services, and e-readers.
- *Cooperate with Competent Authorities*. Upon a national authority's reasoned request, providers must supply all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the AI

Act. Upon reasoned request, providers must also give the authority access to the logs automatically generated by the system to the extent they are under the provider's control.

- *Appoint Authorized Representatives*. Prior to making high-risk AI systems available on the EU market, providers established outside the European Union must appoint an authorized representative established in the European Union. This representative can be addressed, in addition to or instead of the provider, by the competent authorities on all compliance issues. The authorized representative must perform the tasks specified in the written mandate received from the provider. This mandate must empower the representative to carry out the following tasks:
  - Verify that the provider has drawn up the EU declaration of conformity and the technical documentation and has carried out an appropriate conformity assessment procedure.
  - Keep at disposal of the national competent authorities, for 10 years after the system has been placed on the market or put into service, the contact details of the provider, a copy of the EU declaration of conformity, the technical documentation, and, if applicable, the certificate issued by the conformity assessment body.
  - Provide the national competent authority, upon reasoned request, with the requested information and documentation necessary to demonstrate conformity with the requirements for high-risk AI systems set out in the AI Act, including access to the logs automatically generated by the system, provided they are under the provider's control.
  - Cooperate with national competent authorities, upon reasoned request.
  - Comply with the registration obligations—if the registration is carried out by the provider, the authorized representative must ensure that the registration includes the right information.
- *Understand Responsibilities Along the Value Chain*. The provider of a high-risk AI system and the third party that supplies such a system or the tools, services, components, or processes used or integrated in such a system must, through a written agreement, specify the necessary information,

capabilities, technical access, and other assistance based on the generally acknowledged state of the art. The objective is to enable the provider to comply with its obligations. However, this requirement does not extend to third parties offering tools, services, processes, or components to the public, excluding general purpose AI models, under a free and open license.

- *Beware of the Requalification Clause—Deployers and Others May Become Providers*. The AI Act incorporates a requalification clause for high-risk AI systems, wherein any third party, such as a distributor, importer, or deployer, is requalified as a provider and consequently subjected to the obligations of the provider if they engage in certain actions.
  - *In General*. These actions are as follows: putting their name or trademark on a system already placed on the market or put into service in the European Union, making substantial modifications to such a system that maintains its high-risk status, or modifying its intended purpose in a manner that renders it high risk. In such cases, the initial provider is no longer the provider, but it must cooperate with the new one, make available the necessary information, and provide the reasonably expected technical access and other assistance required for the fulfillment of the obligations set out in the AI Act. This is without prejudice to the need to observe and protect intellectual property rights, confidential business information, and trade secrets in accordance with EU and national law. If the initial provider had clearly specified that its AI system is not to be changed into a high-risk system, it does not fall under the obligation to hand over the documentation.
  - *Specific Harmonization Legislation*. In the case of high-risk AI systems that are safety components of products covered by specific EU harmonization legislation listed in the AI Act (e.g., regarding the safety of toys, lifts, radio equipment or medical devices), two actions requalify third parties as providers: the system is placed on the market together with the product under the name or trademark of the manufacturer, or the system is put into service under the name or

trademark of the product manufacturer after the product has been placed on the market.

Obligations for Importers of High-Risk AI Systems

- *Perform Certifications*. Importers are required to make several verifications before placing a high-risk AI system on the market. They must ensure that the provider has carried out a conformity assessment, drawn up the required technical documentation, affixed the required CE marking, provided the EU declaration of conformity and instructions for use, and appointed an authorized representative if applicable.
- *Conclude from Checks*. If verifications give the importer sufficient reasons to consider that the system is not compliant with the AI Act, is falsified or is accompanied by falsified documentation, the importer cannot place the system on the EU market until it is brought into conformity. Importers must inform the provider, the authorized representative, and the market surveillance authorities if the system in question has the potential to adversely affect individuals' health, safety, or fundamental rights to a degree that goes beyond that considered reasonable and acceptable in relation to its intended purpose or under normal or reasonably foreseeable conditions of use.
- *Be Transparent*. Importers must indicate their name, registered trade name or trademark, and address on the system packaging or accompanying documentation, where applicable.
- *Ensure Compliance*. Importers are responsible for ensuring that storage or transport conditions do not compromise the system's compliance with the requirements for high-risk AI systems. This obligation only applies where applicable and while the system is under the importer's responsibility.
- *Keep Documentation*. Importers must keep, for a period of 10 years after the system has been placed on the market or put into service, a copy of the certificate issued by the conformity assessment body, where applicable, of the EU declaration of conformity and instructions for use.

- *Cooperate with Authorities*. Importers must provide to national competent authorities, upon a reasoned request, all the necessary information and documentation to demonstrate the conformity of the system with the AI Act requirements. Importers must also cooperate in any action those authorities take, in particular, to reduce and mitigate the risks posed by the system.

Obligations for Distributors of High-Risk AI Systems

- *Perform Verifications*. Distributors are required to make different verifications before placing a high-risk AI system on the market. They must ensure that the provider has affixed the required CE marking and provided the EU declaration of conformity and instructions for use. In addition, distributors must ensure that the provider and the importer (as applicable) have complied with their obligation to indicate on the system packaging or accompanying documentation their name, registered trade name or trademark, and address. Distributors must also ensure that providers have put in place an appropriate quality management system.
- *Conclude from Checks*. If a distributor has grounds to believe, based on the information available, that the system does not comply with the requirements of the AI Act, it is subject to the same obligations as importers, as outlined above. If the distributor has already made the system available on the market, it must take the corrective actions necessary to bring the system into conformity with the requirements of the AI Act, including withdrawal or recall. Alternatively, the distributor must ensure that the provider, importer, or any relevant operator takes these corrective actions. In cases where the high-risk AI system may adversely affect individuals' health, safety, or fundamental rights (see above), the distributor must immediately inform the provider or importer and the relevant national competent authorities. This notification should include details of the noncompliance and any corrective actions taken.

- *Ensure Compliance*. The same obligations apply to distributors as apply to importers regarding storage and transport of high-risk AI systems.
- *Cooperate with Authorities*. The same obligations apply to distributors as apply to importers.

Notes

* The authors, attorneys with Wilmer Cutler Pickering Hale and Dorr LLP, may be contacted at martin.braun@wilmerhale.com, anne.vallery@wilmerhale.com, and itsiq.benizri@wilmerhale.com, respectively. David Llorens Fernández assisted in the preparation of this article.

1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.

2. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0882.