A&L Goodbody

TECHNOLOGY

Compliance checklist for integrating AI into your business:

12 key compliance questions to consider when integrating AI into your business

If you are a company planning to integrate an AI system into your business, ascertain how the EU's AI Act will impact that process can seem like a difficult and complex task.

16 MIN READ

To assist in simplifying that assessment, this article sets out 12 key questions to consider when integrating AI into your business, which will walk you through the Act's requirements and assist you in determining how best to ensure compliance with the AI Act.

Each question is presented with a "Further context" dropdown option, to help you fully understand the scope of the question and how it relates to the requirements of the Act.[1]

1 Please note, this guide is designed to offer a high-level, practical understanding of the Act's provisions, highlighting key considerations for your business. It is for general informational purposes only and does not constitute comprehensive legal advice. For specific guidance tailored to your business, or to discuss any aspect of the AI Act in more detail, please do not hesitate to contact our expert team at ALG.

"AI systems" vs "AI models"

Please note: Before turning to the 12 key questions, as an initial matter, it is important to outline the distinction that the AI Act makes between "AI systems" and "AI models".

Under the AI Act, there are rules which are applicable to "AI Systems" and rules which are applicable to the development of "AI Models".

"AI Models", as defined under the Act, are the underlying infrastructure which "AI systems" are built upon. As per Recital 97 of the Act, although AI Models are essential components of AI Systems, they do not constitute AI systems on their own. AI Models require the addition of further components, such as for example a user interface, to become "AI systems".

As most standard businesses will likely be looking to integrate the more finalised AI systems, rather than building the more bare AI models, this guide is focused on the rules applicable to AI Systems.

However, if you are unsure as to whether your business may be developing an AI model (as opposed to an AI system) you should reach out to your ALG contact for further advice on the obligations applicable to models.

***Q1. Definition of AI**: Does the technology being considered fall within the definition of "AI system" under the Act?*

Further context: An "AI system" is defined by Article 3 of the Act as:

- a machine-based system
- that is designed to operate with varying levels of autonomy
- that infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions

This definition is intentionally broad and is expressly intended to cover a wide range of AI systems, including both complex generative AI tools and more basic systems utilising simpler techniques, like text matching, knowledge based responding, and decision trees.

Accordingly, most AI systems which businesses may wish to utilise, if they employ some level of autonomy or artificial decision making, will fall within the scope of the definition.

If the answer to Question 1 is "yes" - move to Question 2

***Q.2 Prohibited practices:** Is the AI system intended to be used for any of the 8 prohibited practices under the Act?*

Further context: Under Article 5 of the Act, 8 uses of AI are entirely prohibited. Many of these are unlikely to be relevant to most commercial practices but it is worth double checking at the outset. These 8 practices are listed below (but further detail on each can be found in the *ALG Guide to the AI Act*):

1. **Subliminal, manipulative or deceptive techniques to distort behaviour** (Article 5(1)(a))
2. **Exploitation of vulnerabilities (such as personality traits, age, physical or mental ability) to distort behaviour** (Article 5(1)(b))
3. **Social Scoring leading to unfavourable treatment** (Article 5(1)(c))
4. **Profiling for criminal risk assessment** (Article 5(1)(d))
5. **Creation or expansion of facial recognition databases through scraping** (Article 5(1)(e))
6. **Inference of emotions in working life and education** (Article 5(1)(f))
7. **Biometric categorisation** (Article 5(1)(g))
8. **Real-time remote biometric identification in public spaces** (Article 5(1)(h))

If you have a concern that the proposed use of an AI system may fall within the scope of one of the prohibited practices, you should reach out to your ALG contact for further advice on the relative scope of the prohibition.

If you are confident that the intended use of the relevant AI System will not fall within the scope of any of the prohibited practices, move on to Question 3.

***Q.3 AI literacy requirement**: Have you considered how you will comply with the AI Act's media literacy requirement?*

Further Context: Article 4 of the Act imposes a general requirement on both: (i) the entities that develop any AI systems (defined as "Providers" in the Act); and (ii) the entities which are using any AI system (defined as "Deployers" in the Act).

It requires such entities to take appropriate measures to ensure there is a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf.

This translates practically into an obligation to ensure that employees (or customers in the case of Providers) that are engaging with an AI system are provided with sufficient training on how to appropriately use the system.

If you have any concerns about how to ensure the implementation of the proposed AI system will be accompanied by appropriate training, you should reach out to your ALG contact for further guidance.

If you are happy you have an appropriate AI Literacy programme in place, move on to Question 4.

High risk AI systems

This next set of questions relates to high risk AI systems. This is an important issue as systems which are considered "high risk" under the Act are subject to significant regulatory obligations.

If you are happy that your proposed system is not a "High Risk AI System", you can skip to Question 7.

If you are unsure as to whether the AI system being considered is "high risk" under the Act, Questions 4 – 6 will walk you through the process of determining whether an AI system falls within the scope of the "high risk" provisions, and outline the key regulatory obligations applicable to "high risk" AI systems.

***Q4. High risk AI system identified in Annex I**: Is the proposed AI system either:*

a. itself a product which is subject to the EU product safety harmonisation legislation which is listed in Section A of Annex I of the Act; and

b. part of the safety component of a product which is subject to the EU product safety harmonisation legislation which is listed in Section A of Annex I of the Act?

Further context: Section A of Annex I of the Act, lists 12 pieces of the EU's product safety legislation covering a range of products including: machinery, children's toys, recreational watercrafts, elevators, personal protective equipment, radio equipment, cableway installations, gas fuel appliances, diagnostic and medical devices.

The full list of legislation is outlined below for review:

1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC
2. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys
3. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC
4. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts
5. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres
6. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
7. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment
8. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC
9. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC
10. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC
11. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
12. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU

If the proposed AI system is subject to the relevant harmonisation legislation, you may be subject to the High Risk risk obligations. Move to Question 6 to consider what obligations may apply.

If the proposed AI system is not subject to the harmonisation legislation, move to Question 5.

Q5. High risk AI system identified in Annex III:
Is the proposed AI system intended to operate in one of the "high risk" areas identified to Annex III?

Further context: Annex III of the Act identifies 8 broad, general areas where the use of AI could affect critical areas of society and/or have a significant impact on areas like health, safety or fundamental rights.

Some of the areas identified in Annex III will be of little relevance to businesses. For example, the use of AI systems in the context of law enforcement or border control are both considered to be "high-risk" areas.

However, some of the high-risk areas identified in Annex III may be of keen relevance for certain businesses. These are as follows:

- **Employment and workers management**: AI systems used: for recruitment or employee selection, including for placing targeted job advertisements, screening or filtering applications and evaluating candidates; or
  - to make decisions affecting work related relationships, including, promotion and termination, task allocation, or for monitoring and evaluating performance
- **Enjoyment of essential services:** AI systems used:
  - to evaluate the creditworthiness of individuals
  - for risk assessment and pricing in relation to life and health insurance
- **Critical infrastructure** - AI systems used as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating, and electricity
- **Biometrics** - AI systems used for: remote biometric identification; biometric categorisation according to sensitive or protected characteristics; or emotion recognition systems.(Notably this category does not include AI systems used for biometric verification whose sole purpose is to confirm that a specific natural person is the person he or she claims to be).
- **Education and training** - AI systems used to evaluate learning outcomes or assess the appropriate level of education for an individual

If the proposed AI system will be used in connection with one of the high risk areas identified in Annex III (even if that is not its sole purpose), you may be subject to the High Risk Obligations. Move to Question 6 to consider what obligations may apply.

If the proposed AI system will not be used in respect of the above high risk areas in Annex III, and the answer to Question 4 was also no - the High Risk Obligations will not apply and you can skip to Question 7.

High risk obligations

In order to determine what obligations are applicable, it must first be determined whether the business falls within any of the categories of "Operator" identified under the Act.

Q.6. Type of operator for high risk AI: *Which of the following applies to your intended use of the proposed AI System:*

A. *Will the business be:*

- *developing the relevant AI system itself,*
- *making substantial modifications to an existing AI system,*
- *modifying the intended purpose of an existing AI system or*
- *placing an existing AI system on the market under the business' own name or trademark?*

B. *Will the business be actively using the relevant AI system under its own authority?*

Further context: The Act imposes obligations for different categories of actor in the AI system production and deployment chain (collectively referred to as "Operators" in the Act).

These categories of Operator are:

- **Providers** - which develop the relevant High Risk AI System
- **Deployers** - which use the the relevant High Risk AI System
- **Importers** - which place a High Risk AI System on the EU market that bears the name or trademark of a natural or legal person established outside the EU
- **Distributors** - which are any person in the supply chain, other than the Provider or the Importer, that makes an AI system available on the EU market

The type and extent of obligations which apply in respect of a high risk AI system will depend on the category of Operator a business falls into.

This note is aimed at companies which are looking to integrate AI systems into their businesses so we have limited its focus to Providers and Deployers - but further information on the obligations of Importers and Distributors can be found in the *ALG Guide to the AI Act*)

If you selected "**A**" above, you may be operating as a "**Provider**" of a high risk AI system under the Act. The most onerous obligations in respect of HRAI Systems are placed on Providers. [This encompasses implementing and maintaining certain standards in respect of quality management systems, conformity assessments, incident reporting, documentation and event logging.]

If you selected "**B**" above, you may be operating as a "**Deployer**" of a high risk AI system under the Act. A Deployer's High Risk AI Obligations under the Act are not as extensive as that of a Provider. [In general Deployers must operate an HRAI system in line with its instructions for use and the Act requires Deployers to assist Providers in the Provider's continued monitoring of the system. The Act also identifies specific obligations for Deployers in respect of input data and providing certain information to natural persons who may be affected by the use of the system].

The below table provides links to a full summary of the obligations applicable to each type of Operator.

Option	Type of Operator under the AI Act	Relevant Obligations
A.	Provider	Summary of obligations
B.	Deployer	Summary of obligations

Please note that it is possible for a business to constitute both the Provider and the Deployer in respect of the same AI system.

General transparency obligations

Regardless of whether an AI system falls within the "high risk" category or not, there are certain transparency obligations which will apply where an AI system is used for certain, specific purposes. Before looking at those transparency obligations, it is again relevant to understand what type of Operator the business may be acting as:

*Q7. **Type of operator:** Which of the following applies to your intended use of the proposed AI System:*

A. *Will the business be developing the relevant AI system itself?*

B. *Will the business be actively using the relevant AI system under its own authority?*

If you selected "**A**" above, you may be operating as a "**Provider**" under the Act.
Go to Question 8 and 9 for more information on potential obligations as Provider.

If you selected "**B"** above, you may be operating as a "**Deployer**" under the Act.
Go to Question 10, 11 and 12 for more information on potential obligations as Deployer.

Q8. Direct interaction: Is the proposed AI system intended to interact directly with natural persons (e.g. a chat bot which responds to customer queries)?

Further context:. The Act imposes a general obligation for Providers to ensure that natural persons interacting with an AI system are made aware that they are interacting with an AI system.

When implementing that obligation, the characteristics of natural persons belonging to vulnerable groups due to their age or disability should be taken into account if the AI system is intended to interact with those groups as well.

Natural persons should also be notified when they are exposed to AI systems that, by processing their biometric data, can identify or infer the emotions or intentions of those persons or assign them to specific categories. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, personal traits, ethnic origin, personal preferences and interests. Such information and notifications should be provided in accessible formats for persons with disabilities.

If the answer to Question 8 is yes, the Providers of such an AI system must ensure they are designed in such a way that the relevant natural persons should reasonably be made aware that they are interacting with an AI system.

This could be a simply worded disclaimer message which appears when the system is being used, informing users that they are engaging with AI. The disclaimer language should take account of the likely audience for such a message.

Q9. Content as created by AI: *Can the proposed AI system generate synthetic audio, image, video or text content?*

Further context: Many AI Systems can produce synthetic content which is difficult to to distinguish from human-generated content. The Act imposes a general obligation on the Providers of such systems to embed technical solutions that enable the content to include some form of marking in a machine readable format which allows for the easy detection that the output has been generated or manipulated by an AI system and not a human.

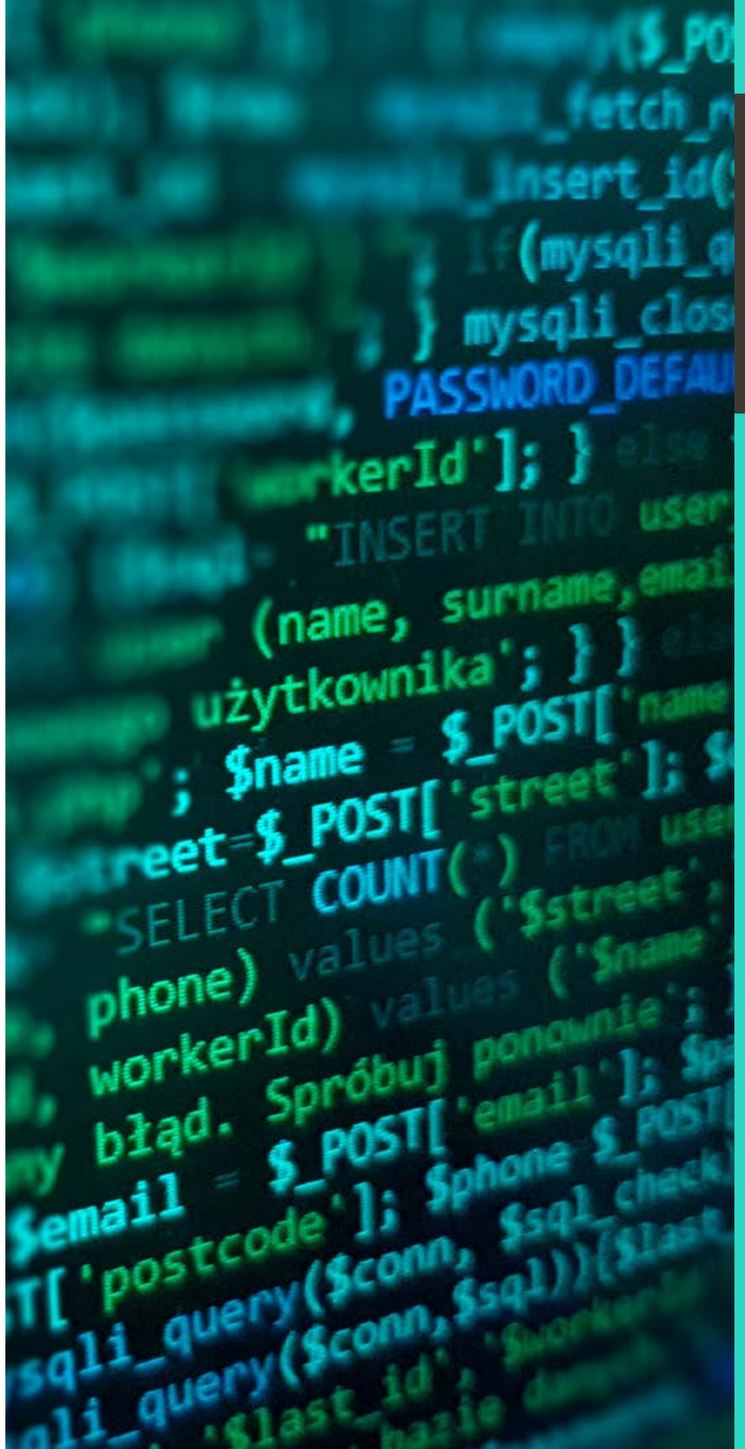
As per Recital 133, the Act requires that such “marking” techniques and methods should be sufficiently reliable, interoperable, effective and robust as far as this is technically feasible, taking into account available techniques or a combination of such techniques, such as watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, fingerprints or other techniques, as may be appropriate.

When implementing this obligation, providers should also take into account the specificities and the limitations of the different types of content and the relevant technological and market developments in the field, as reflected in the generally acknowledged state of the art. Such techniques and methods can be implemented at the level of the AI system or at the level of the AI model, including general-purpose AI models generating content, thereby facilitating fulfilment of this obligation by the downstream provider of the AI system.

To remain proportionate, this marking obligation is not intended to cover AI systems performing primarily an assistive function for standard editing or AI systems not substantially altering the input data provided by the Deployer.

If the answer to Question 9 is yes, the Provider of such an AI System must ensure that such outputs of the system are marked in a machine-readable format and detectable as artificially generated or manipulated.

This obligation does not apply to the extent the AI systems perform an assistive function for standard editing or does not substantially alter the input data.



***Q10. Emotion recognition or biometric categorisation**: Will the proposed AI system be used for the purpose for emotion recognition or biometric categorisation?*

Further context: As per Recital 16, the notion of **'biometric categorisation**' referred to in the Act should be understood as assigning natural persons to specific categories on the basis of their biometric data. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or, interestingly, political orientation.

It does not include biometric categorisation systems that are a purely ancillary feature which is intrinsically linked to a commercial service, whereby the feature cannot be used without the principal service, and the integration of that feature or functionality.

For example, filters categorising facial or body features used on online marketplaces (e.g. searching for clothes in a "medium" size) could constitute such an ancillary feature as they can be used only in relation to the principal service which consists in selling a product by allowing the consumer to preview the display of the product on him or herself and help the consumer to make a purchase decision.

Filters used on social media services which categorise facial or body features to allow users to add or modify videos (e.g. a "cat's eyes" filter) could also be considered an ancillary feature as such a filter cannot be used without the principal service of the social media service consisting in the sharing of content online.

As per Recital 18, the notion of an **'emotion recognition system**" should be understood as an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data.

The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement.

It does not include physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for thepurpose of preventing accidents.

It also does not include the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering.

If the answer to Question 10 is yes, the Deployers of such systems must inform the natural persons exposed to the system of its operation, and must ensure that all personal data processed is done in accordance with the GDPR and EU data protection rules.

***Q11. Deep fakes**: Is the proposed AI system capable of generating image, audio or video content constituting a "deep fake"?*

Further context: The Act imposes specific obligations on Deployers who use an AI system to generate or manipulate "deep fake" content - i.e. image, audio or video content that appreciably resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.

Deployers must clearly and distinguishably disclose that the content has been artificially created or manipulated by labelling the AI output accordingly and disclosing its artificial origin.

Per Recital 134, compliance with this transparency obligation should not be interpreted as indicating that the use of the AI system or its output impedes the right to freedom of expression, in particular where the content is part of an evidently creative, satirical, artistic, fictional or analogous work or programme.

In those cases, the transparency obligation for deep fakes is limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work, including its normal exploitation and use, while maintaining the utility and quality of the work.

If the answer to Question 11 is yes, the Deployer of such a system must clearly disclose that the content has been artificially generated or manipulated.

***Q12. Matters of public interest**: Is the proposed AI system used to generate or manipulate text which is published for the purpose of informing the public on matters of public interest?*

Further context: The Act also imposes a specific obligations on Deployers who use an AI system to produce AI-generated or manipulated text which is published with the purpose of informing the public on matters of public interest - e.g. an industry newsletter which is produced and circulated solely by AI.

However if AI-generated content which has undergone a process of human review or editorial control and a natural or legal person holds editorial responsibility for the publication of the content, it will fall outside the scope of this obligation. So if that industry newsletter was reviewed and finessed by a human employee before being circulated, it should fall outside this scope.

If the answer to Question 12 is yes, the Deployer of such a system must clearly disclose that the text has been artificially generated or manipulated. This again could be done by way of a disclaimer provided at the point of providing the AI generated content.

This obligation shall not apply where the AI-generated content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication

A&L Goodbody

Key contacts

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Aideen Burke
Partner
+353 1 649 2627
aiburke@algoodbody.com

Chris Bollard
Partner
+353 1 649 2328
cbollard@algoodbody.com

Stephen King
Partner
+353 1 649 2243
sking@algoodbody.com

Andrew Sheridan
Partner
+353 1 649 2766
asheridan@algoodbody.com

Evan Doyle
Senior Associate
+353 1 649 2753
evdoyle@algoodbody.com

Resources

Gov.ie – Dept Enterprise – the EU Artificial Intelligence Act	READ MORE
EU Commission AI Act FAQs	READ MORE
EU Commission AI Literacy Obligation FAQs	READ MORE
EU Commission Guidelines on Prohibited AI Practices	READ MORE
EU Commission Guidelines on definition of AI System	READ MORE