Hey 👋

I'm Oliver Patel, author and creator of ***Enterprise AI Governance***.

This free newsletter delivers practical, actionable, and timely insights for AI governance professionals.

My goal is simple: to empower you to understand, implement, and master AI governance.

If you haven't already, sign up below and share it with your colleagues. Thank you!

This two-part series on *Enterprise AI Governance* presents and debunks 10 common misconceptions about the AI Act, providing a detailed explanation for each one. The first 5 **were covered in part 1** and the second 5 are covered in this edition.

The ten misconceptions are:

1. The EU AI Act has a two-year grace period and applies in full from August 2026.
2. All open-source AI systems and models are exempt from the EU AI Act.
3. High-risk AI models are explicitly regulated under the EU AI Act.
4. Emotion recognition is prohibited under the EU AI Act.
5. Facial recognition is prohibited under the EU AI Act.
6. Transparency is required for 'limited risk' AI systems.

7. Third-party conformity assessments are required for all high-risk AI systems.
8. Fundamental rights impact assessments are required for all high-risk AI systems.
9. All high-risk AI systems must be registered in the public EU-wide database.
10. Deployers do not need to register their use of high-risk AI systems.

👨‍🎓 If you want to dive much deeper, register interest for my **EU AI Act Compliance Bootcamp** here**.** This will be an exclusive and intimate masterclass for AI governance leaders, breaking down how to implement AI Act compliance in an enterprise setting. More information will be shared later in the year.

Note: *if you already registered interest for my AI Usage Policy Bootcamp, you do not need to register here again. Stay tuned for further info.*

Misconception 6. Transparency is required for 'limited risk' AI systems.

This is an important example, because the AI Act does not use the term 'limited risk' to refer to the AI systems for which transparency is required. Therefore, it does not make sense to use this term. It would be like using completely different and inappropriate terminology when referring to 'high-risk AI systems' or 'prohibited AI practices'.

What the AI Act *actually* says is that for certain AI systems, there are transparency obligations for providers and deployers. Therefore, more accurate terminology than 'limited risk' is 'transparency requiring AI systems'. It may not roll off the tongue as smoothly, but it does the job.

All the AI Act risk pyramid images which are widely circulated (including sometimes by EU departments), which use the term 'limited risk' instead of 'transparency requiring' (or something of that nature) are arguably fuelling this misconception.

This misconception has taken hold due to a lack of precision regarding the language which is used to talk about the AI Act. This is problematic, because in a complex legal text like this, there are many different terms which, although they may sound conceptually similar, mean different things and can give rise to very different real-world consequences.

To accurately and effectively understand, interpret, and comply with a law of this complexity, precision and care with language is key.

Article 50 outlines the transparency obligations for certain AI systems. The AI systems are:

- AI systems intended to interact directly with people;
- AI systems that generate synthetic image, audio, video or text content;
- emotion recognition systems;
- biometric identification systems; and
- AI systems which generate or manipulate deep fake content.

Providers and deployers of these AI systems are obliged to implement additional transparency measures, such as notification and disclosure, which are detailed in Article 50.

These ‘transparency requiring AI systems’ can simultaneously be high-risk AI systems, or AI systems which are not high-risk. In the former scenario, all applicable obligations and requirements for high-risk AI systems would also apply. In the latter scenario, only the transparency obligations in Article 50 would apply.

This is another reason why the ‘classic’ yet misleading AI Act risk pyramid doesn’t

work: it falsely implies that the obligations for high-risk AI systems and 'transparency requiring AI systems' are mutually exclusive.

This point has been observed and elaborated on by other analysts, such as Aleksandr Tiulkanov, who has produced two helpful infographics to help conclusively debunk this misconception.

See below for the two original images, which have not been modified, and were posted on Aleksandr's article 'EU AI Act: Getting the Basics Straight'.

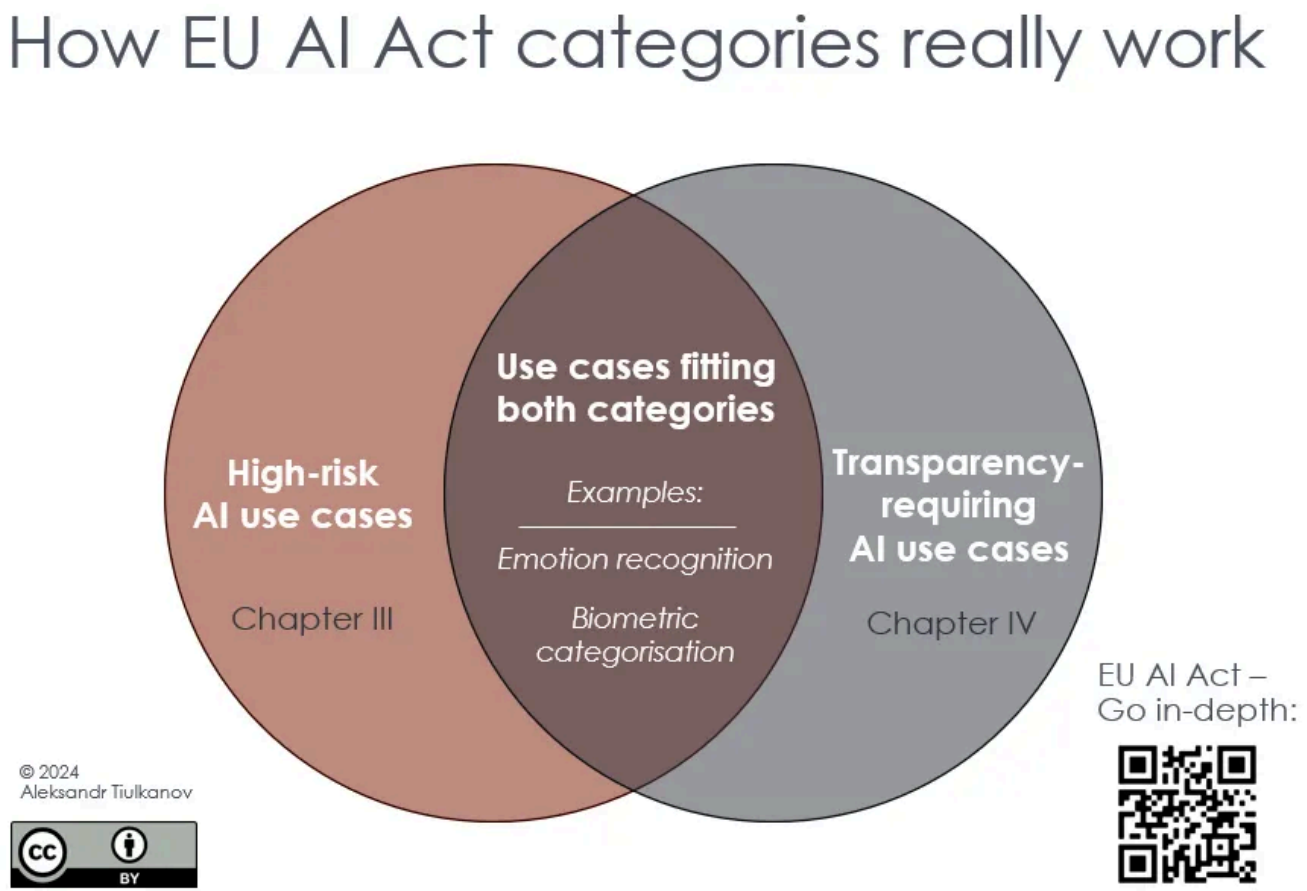
Meaning of “Limited risk”

Limited risk AI use cases ≠ **Transparency-requiring use cases**

Limited risk AI use cases = **Potential high-risk AI use cases that are exempt**

Recital 53, Art 6(3) AIA

EU AI Act – Go in-depth:



Misconception 7: Third-party conformity assessments are required for all high-risk AI systems

Under the AI Act, providers are obliged to ensure that their high-risk AI systems undergo a conformity assessment before they are placed on the market or put into service.

A conformity assessment is an established and longstanding practice for many products regulated by EU product safety laws.

The AI Act defines a 'conformity assessment' as "*the process of demonstrating whether the requirements set out in Chapter III, Section 2 relating to a high-risk AI system have been fulfilled*". This means the focus of the conformity assessment is largely on the following requirements:

- risk management system,
- data and data governance;
- technical documentation;
- record-keeping;
- transparency and provision of information to deployers;
- human oversight; and
- accuracy, robustness and cybersecurity.

Once the conformity assessment is completed, the provider must produce the 'declaration of conformity', which can be inspected by other parties, like importers or distributors.

However, not all high-risk AI systems are obliged to undergo the same conformity assessment procedure. The key distinction is between the two main categories of high-risk AI system:

1. AI systems which are products, or safety components of products, regulated by one of the EU product safety laws listed in Annex I; and

2. AI systems listed in Annex III.

For the first category of high-risk AI system, the requirement to undergo a third-party conformity assessment is already stipulated in the existing laws which are referenced in Annex I. Moreover, the AI systems covered by these existing laws are not classified as high-risk under the AI Act **unless** the relevant product is already required to undergo a third-party conformity assessment.

To avoid burdensome and duplicative compliance work, the AI Act does not create a new and additional conformity assessment regime for these AI systems.

What it says is that the existing conformity assessment procedure, performed by a third-party (i.e., a notified body) must continue to be followed, but that it must also

now consider and include the new requirements outlined in the AI Act. This necessarily entails an update to, and augmentation of, those existing third-party conformity assessment procedures.

However, for the second category of high-risk AI systems (i.e., those listed in Annex III), there is no obligation for a third-party conformity assessment. Rather, providers must perform a 'self-assessment', which does not involve a third-party (i.e., a notified body).

Article 43(2) refers to this as the "*conformity assessment procedure based on internal control*". Annex VI provides further information about how providers must perform this self-assessment.

EU legislators opted for this approach due to the lack of AI certification expertise and maturity in the wider market, which was deemed an impediment to notified bodies performing conformity assessments across all these domains, at least for now. However, Recital 125 suggests that in future, as the market matures, these conformity assessments may also be performed by notified bodies.

The only partial exception to this is high-risk AI systems used for biometrics, including:

- remote biometric identification;
- biometric categorisation; and

- emotion recognition.

In certain scenarios, a third-party conformity is required for these high-risk AI systems. For example, if the provider has not fully applied an official technical standard to demonstrate compliance, or if such a standard does not exist, then the conformity assessment must be performed by a notified body. The procedure for this is outlined in Annex VII.

Misconception 8: Fundamental rights impact assessments are required for all high-risk AI systems

Performing a fundamental rights impact assessment is an important obligation which applies to certain deployers of specific high-risk AI systems.

Where applicable, a fundamental rights impact assessment must be performed by the deployer prior to using the AI system.

The fundamental rights impact assessment is a formal exercise where deployers must consider, describe, and document how and when they will use the AI system, which people or groups will be impacted by it, the specific harms likely to impact those

people, how human oversight will be implemented, and what will be done by the deployer if any risks materialise or harm arises.

It does not apply to providers, nor does it apply to all deployers or all high-risk AI systems.

The obligation only applies to the following deployers:

- bodies governed by public law;
- private entities providing public services;
- deployers of AI systems used for life and health insurance risk assessment and pricing; and
- deployers of AI systems used for creditworthiness evaluation and credit score assessment.

For the deployers which are governed by public law, or private entities providing public services, they must only perform a fundamental rights impact assessment before using one of the high-risk AI systems in Annex III. However, this excludes AI systems used for safety management and operation of critical infrastructure, for which no fundamental rights impact assessment is required.

In practice, this means that most businesses will not have to perform a fundamental rights impact assessment prior to using a high-risk AI system. This is either because it does not apply to them as a deployer, or it does not apply to the high-risk AI system they are using, or both.

However, for some financial services and insurance firms, as well as companies which provide AI-driven public services in domains like welfare, education, and border control, this will become an important part of their AI governance and compliance work.

Once the fundamental rights impact assessment has been completed, the deployer must notify the relevant regulator and, if applicable, summarise its findings in their registration entry in the EU database for high-risk AI systems (*see misconception 10 below*).

Whilst providers of all high-risk AI systems are required to perform risk assessments and implement risk management measures (see Article 9)—which includes considering the potential risk to fundamental rights—this is not the same as a dedicated fundamental rights impact assessment.

Misconception 9: All high-risk AI systems must be registered in the public EU-wide database

Article 71 of the AI Act mandates the European Commission to establish and maintain an EU database for high-risk AI systems. It must be "*publicly accessible, free of charge, and easy to navigate*".

Providers of certain high-risk AI systems are obliged to register information about their AI systems and their organisation in this database. They must do this before placing the high-risk AI system on the market or putting it into service.

To dispel this misconception, there are four important points you should understand, each of which are explained below:

1. The registration obligation does not apply to all high-risk AI systems.
2. The registration obligation applies to some AI systems which are not technically high-risk.
3. Not all information in the database will be available to the public.
4. Some high-risk AI systems must be registered in a national database, instead of the EU database.

1. The registration obligation does not apply to all high-risk AI systems

The registration obligation, outlined in Article 49, only applies to high-risk AI systems listed in Annex III. This includes AI systems used for recruitment, health insurance pricing, and educational admissions.

However, this excludes AI systems which are products, or safety components of products, regulated by one of the EU safety laws listed in Annex I. This means that AI systems used in critical, regulated domains, like medical devices, vehicles, and aviation do not need to be registered in the EU's public database.

There are various other ways in which the AI Act compliance obligations and requirements differ across these two main categories of high-risk AI system, such as with respect to conformity assessments (*as outlined in misconception 7 above*).

2. The registration obligation applies to some AI systems which are not technically high-risk

Article 6(3) specifies an important caveat for the classification of high-risk AI systems. It states that high-risk AI systems listed in Annex III are **not high-risk** if they do not "*pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making*".

Four potential conditions are provided. If one of these is met, then the AI system does

not pose this type of risk and is thus not classified as high-risk. For example, one condition is that the AI system performs only a "*narrow procedural task*".

Interestingly, even where a provider legitimately determines—as per the Article 6(3) exception procedure—that their AI system is not high-risk, they must still register that AI system in the EU's public database.

The logic of this is to promote transparency regarding how providers are determining and documenting that AI systems are not high-risk, despite being used in sensitive (Annex III) domains.

This could lead to a potentially vast number of AI systems needing to be registered and many organisations being unaware that they are obliged to do so.

3. Not all information in the database will be available to the public

For certain high-risk AI systems listed in Annex III, including AI systems used for law enforcement, migration, asylum, and border control management, the information will be registered and stored in a "*secure non-public section*" of the EU database.

This includes lawful AI systems used for remote biometric identification, biometric categorisation, and emotion recognition, in the context of law enforcement, migration, asylum, and border control management.

These providers are obliged to register less information than the providers of the other high-risk AI systems, and that information can only be viewed by the European Commission and the specific member state regulators who have been designated to lead on AI Act enforcement for those sensitive sectors.

Therefore, many of the AI systems which are the most sensitive, and arguably pose the greatest risk to fundamental rights, will not be publicly registered.

4. Some high-risk AI systems must be registered in a national database, instead of the EU database.

Providers of high-risk AI systems that are used as safety components for the operation and management of critical infrastructure, like water and energy, are obliged to register their AI systems, and themselves, at the "national level".

This means that the registration of these AI systems will be in different databases—maintained by member state regulators and/or governments—separate from the public database maintained by the European Commission.

The AI Act does not reveal much about these national level databases. However, there is no provision which states that they must be public. This signals an acknowledgement of the sensitivity and secrecy of these domains, because of their importance to national security and economic stability.

Misconception 10: Deployers do not need to register their use of high-risk AI systems

Certain deployers of specific high-risk AI systems are also obliged to register information about their organisation, and the high-risk AI system they are using, in the EU database. They must do this before using the AI system.

This obligation only applies to deployers that are "*public authorities, EU institutions, bodies, offices or agencies or persons acting on their behalf*".

The focus is therefore on public sector organisations in the EU using high-risk AI, as opposed to private sector and commercial AI usage.

These organisations must register themselves, and select which high-risk AI system they are using, in the EU database. It will not be possible to do this if the provider has not already registered the high-risk AI system. Therefore, this is something which should be checked by the deployer, as part of procurement and partnership due diligence.

This also means that the deployer registration obligation only applies to the high-risk AI systems which providers are obliged to register. This includes the high-risk AI

systems used for law enforcement, migration, asylum and border control management, however the deployer information will also be registered the "*secure non-public section*" of the EU database, which only the European Commission and certain public authorities can access.

There is no explicit provision which stipulates that deployers must register their use of AI systems used for critical infrastructure safety management and operation, which providers must register at the national level instead of the EU-wide database.

There is also nothing which indicates that deployers are obliged to register their use of AI systems which are not high-risk, but have nonetheless been registered as they fell under the scope of an Article 6(3) derogation.

Finally, there are certain scenarios when deployers can become providers of high-risk AI systems, either intentionally or inadvertently. For example, if they make a "substantial modification" to the AI system and it remains high-risk. In these scenarios, the new provider would be required to register the high-risk AI system.

👨‍🎓 If you found this post useful, register interest for my **EU AI Act Compliance Bootcamp** here**.** This will be an exclusive and intimate masterclass for AI governance leaders, breaking down how to implement AI Act compliance in an enterprise setting.