

General-Purpose AI Model Compliance Guide (Part 1)



Edition #25
By Oliver Patel

ENTERPRISE AI GOVERNANCE



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!

Follow me on LinkedIn for more frequent updates.

It has been a consequential few weeks for the EU AI Act's provisions on general-purpose AI (GPAI) models.

Now that we've all had some time to (hopefully) take a deep breath, relax, and take stock, it is the ideal moment for a deep-dive on GPAI model compliance.

The next three editions of Enterprise AI Governance will provide a comprehensive, practical, and actionable GPAI Model Compliance Guide. It is targeted at AI governance, legal, and compliance practitioners working for firms that develop, fine-tune, modify, deploy, or otherwise use GPAI models. That is quickly encompassing all of us.

My goal is to simplify these complex obligations and highlight what they mean for your business.

Note: *this series assumes familiarity with the EU AI Act, its core concepts, and the topic of general-purpose AI and foundation models more broadly.*

Part 1's focus (this edition) is on **Obligations for Providers of GPAI Models**. It covers:

- ✓ What is a GPAI model?
- ✓ What do providers of GPAI models need to do?
- ✓ What about open-source GPAI models?
- ✓ What about legacy GPAI models (released before 2 August 2025)?
- ✓ How does the GPAI Code of Practice fit in?
- ✓ How and when will the GPAI model provisions be enforced?

And here is a glimpse of what's coming in parts 2 and 3.

Part 2 will focus on **GPAI Models with Systemic Risk**, covering:

- ✓ What is a GPAI model with systemic risk?
- ✓ How are such models classified and what are the exemptions?
- ✓ What do providers of GPAI models with systemic risk need to do?

- ✓ How do the compliance obligations differ?
- ✓ Deep dive on the GPAI Code of Practice: Safety and Security Chapter

And Part 3 wraps up the series with the question on everyone's lips: am I a GPAI model provider!?

The focus here will be on '**Downstream Actors': Modification, Deployment, and Use of GPAI Models**:

- ✓ Who exactly is a provider of a GPAI model?
- ✓ How do you become the provider of a GPAI model you are modifying?
- ✓ What is a 'downstream provider' and how do you become one?
- ✓ What is a general-purpose AI system?
- ✓ What if you integrate a GPAI model into a high-risk AI system?
- ✓ How should you assess GPAI model providers and choose which models to use?

By the end of the series, you will have a thorough understanding of precisely what your organisation needs to do to achieve compliance. My analysis represents a simplified breakdown of the following official legal and regulatory documents, which are referenced throughout.

- EU AI Act full text
- European Commission Guidelines for Providers of GPAI Models

- GPAI Code of Practice
 - Transparency Chapter
 - Model Documentation Form
 - Copyright Chapter
 - Safety and Security Chapter
- Template for publishing GPAI Model Training Data Summary

The aforementioned Code of Practice, Guidelines, and Training Data Template were all published in July 2025. And the Code of Practice was formally approved by the EU on 1 August 2025, one day before the GPAI model provisions became applicable on 2 August 2025.

What is a GPAI model?

Whether or not you are a provider of a GPAI model, and thus subject to the below obligations, depends on whether or not the model you are developing and placing on the market is in fact a GPAI model.

The AI Act defines a GPAI model as:

*"An AI model, including where such an AI model is **trained with a large amount of data** using **self-supervision at scale**, that displays **significant generality** and is capable of **competently performing a wide range of distinct tasks** regardless of the way the model is placed on the market and that can be **integrated into a variety of downstream systems or applications**, except AI models that are used for research, development or prototyping activities before they are placed on the market".*

The corresponding AI Act recital says that models with at least 1 billion parameters, trained in this way, should be considered to be GPAI models.

In its recent guidelines, the European Commission acknowledged that the above definition is fairly general and lacks specific, objective criteria that organisations can use to determine whether or not their models constitute GPAI.

Plugging this gap, the Commission has now provided specific criteria for GPAI model classification. This criteria is based on the amount of computational resource used to train the model.

Specifically, if a model's training compute is greater than 10^{23} floating-point operations (FLOP) and it can generate language (either text or audio), or generate image or video based on text inputs, then it should be considered a GPAI model.

The Commission's position is that there is a direct correlation between how much computational resource is used to train the model—which in itself is linked to the size of the model and the volume of training and pre-training data—and the general-purpose capabilities of the model.

However, it is acknowledged that there could be exceptional instances where a model trained with this amount of computational resource that generates text would not meet the legal definition of a GPAI model (e.g., if it did not display significant generality in its capabilities). Also, a model which does not meet this indicative criteria may also meet the legal definition of a GPAI model.

The key message is that organisations developing and fine-tuning large AI models at scale need to track the computational resource they use in a standardised and automated way.

What do providers of GPAI models need to do?

Providers of GPAI models are organisations or entities that develop such AI models and place them on the market or otherwise make them available.

Part 3 of this series will cover exactly who is a provider of a GPAI model and how to know if you are one. For now, here are some examples the European Commission provides that constitute a provider placing a GPAI model on the market. In all instances, company A is the GPAI model provider.

- Company A develops a GPAI model and makes it available via a software library, repository, API, or cloud computing service.
- Company A commissions company B to develop a GPAI model on its behalf, and company A makes it available via a software library, repository, API, or cloud computing service.
- Company A develops a GPAI model and uploads it to an online repository hosted and managed by company C.

There are a suite of obligations that apply to providers of all GPAI models, as well as additional obligations that also apply to providers of GPAI models with systemic risk. Part 2 of this series will cover, in detail, the obligations for providers of GPAI models with systemic risk. They are left out here.

Below is a summary of the four main sets of obligations that apply to providers of *all* GPAI models:

1. Providers of GPAI models must develop, maintain, and keep up-to-date

comprehensive technical documentation which provides information about the GPAI model, how it was developed, and how it should be used.

- The Transparency Chapter of the GPAI Code of Practice provides extensive detail about how this can be done. It is accompanied by a Model Documentation Form consisting of 42 metadata attributes across 8 categories. This builds on the elements set out in Annex XI and XII of the AI Act.
- The attributes include training time and computation, model size, energy consumption, data collection and curation methods, and input and output modalities.
- Some of this information must be shared with the European Commission's AI Office and/or national regulators (on request), and some must be proactively shared with 'downstream providers', which are organisations that integrate GPAI models into an AI system.
- Some documentation is required for all GPAI models, whereas certain additional documentation is only required for GPAI models with systemic risk.

2. Providers of GPAI models must produce and make publicly available a detailed summary of the content and data used to train the GPAI model.

- The AI Act requires this training data summary to be "sufficiently detailed" and structured in line with a template provided by the AI Office. That template was

published by the European Commission in July 2025, alongside explanatory guidance.

- The template carefully attempts to balance protecting trade secrets and confidentiality with promoting transparency, data protection, and copyright protection.
- In a nutshell, the training data summary should cover the amount and type of training data used, as well as the use of:
 - publicly available datasets;
 - private non-publicly available datasets;
 - data crawled and scraped from online sources;
 - user data; and
 - synthetic data.
- Importantly, the template does not require providers to publish or disclose details about the specific data and works used to train GPAI models, as this would *"go beyond the requirement to provide a 'summary'"*.

3. Providers of GPAI models must implement a policy to comply with EU copyright and intellectual property law.

- Given the large volume of copyright protected material typically used to train GPAI models, this obligation is significant. It compels providers to consider and document how they will comply with EU copyright law in such contexts.
- The AI Act provides minimal detail about how to do this. However, it does stipulate that "state-of-the-art technologies" must be used to promote copyright compliance in the context of developing GPAI models.
- The Copyright Chapter of the GPAI Code of Practice provides more detail, outlining six practical measures for organisations to implement.

4. Providers of GPAI models must cooperate with the European Commission and regulatory authorities and appoint an EU-based authorised representative if they are based outside of the EU.

- The AI Act has extraterritorial effect. In this context, it means that if a provider places their GPAI model on the market or makes it available in the EU, then that provider must comply with the AI Act, irrespective of where the provider is established or operating from.
- In such extraterritorial scenarios, the appointment of an authorised representative is important, to enable effective cooperation and correspondence with the AI Office and any other relevant authorities.

What about open-source GPAI models?

The AI Act exempts providers of open-source GPAI models from the first and fourth set of obligations. Namely, they do not need to develop, maintain, and keep up-to-date comprehensive technical documentation referenced in point 1 above. And they do not need to appoint an authorised representative (if based outside the EU), as referenced in point 4.

However, providers of open-source GPAI models are obliged to comply with points 2 and 3. This means they must implement a copyright compliance policy and publish the training data summary.

Furthermore, providers of open-source GPAI models with systemic risk are not exempt from any of these obligations. This means that they must comply with the obligations for both *all* GPAI models and the additional obligations for GPAI models with systemic risk.

The European Commission's guidelines provide clarity about what exactly constitutes an open-source GPAI model—a hotly contested topic. Here is a summary of the recent guidance:

- To qualify as open-source, a GPAI model must be released under a free and open-source licence that permits unrestricted access, use, modification, and distribution without payment or significant limitations.
- All model parameters, architecture, and usage information must be publicly available to ensure usability.
- A licence is not considered open-source if it includes restrictions like non-commercial use only, prohibitions on distribution, usage limits based on scale, or requirements for separate commercial licences. Essentially, most usage restrictions, aside from those justifiably designed to protect users or other groups, or ensure appropriate attribution, would likely disqualify a GPAI model from open-source classification.
- Monetisation generally also disqualifies a model from open-source exemptions if payment is required for core access, use, or essential, indistinguishably linked support, or if it's exclusively hosted on paid platforms.
- However, optional paid services that don't hinder free use are permissible.

What about 'legacy' GPAI models (released before 2 August 2025)?

Irrespective of when a GPAI model was developed and placed on the market, providers of that model must eventually comply with the AI Act's obligations.

This means that the full suite of obligations, including publishing training data summaries, implementing a copyright compliance policy, and maintaining technical documentation, applies to both 'legacy' and 'new' GPAI models. The only difference is the applicable date of those obligations. For the 'legacy' GPAI models, placed on the market before 2 August 2025, providers have until 2 August 2027 to comply with the aforementioned provisions. For GPAI models released after 2 August 2025, there is no longer a grace period.

The practical implication of this is that virtually all GPAI models that have already been released and made available in the EU will have to retrospectively become compliant. This represents a practical and operational headache for AI developers, especially given how recently the Code of Practice and guidelines about *how* to comply were released.

The European Commission acknowledges that this is going to be challenging, noting that *"the AI Office is dedicated to supporting providers in taking the necessary steps to comply with their obligations by 2 August 2027"*.

However, the Commission confirmed that providers of 'legacy' GPAI models will not have to conduct "retraining or unlearning of models" where this is not possible or

where it would cause undue burden. The Commission accepts that information about historical training data may not always be available and encourages providers to be open about this.

How does the GPAI Code of Practice fit in?

The GPAI Code of Practice was published by the European Commission on 10 July 2025 and was approved by the EU on 1 August 2025.

The AI Act mandated the Commission to work with external experts to develop the Code of Practice, to assist GPAI model providers in their compliance journey.

It is a voluntary tool which helps providers comply with the full suite of obligations for GPAI models. Although organisations are not obliged to sign and implement the Code of Practice, doing so provides a standardised and endorsed approach for regulatory compliance. This offers more legal certainty regarding the validity of an organisation's approach.

However, you can still be compliant, via adequate alternative means, even if you do not sign up to and follow the Code of Practice.

The Code of Practice consists of three chapters: 1) Transparency, 2) Copyright, and 3) Safety and Security. Each chapter contains several 'measures'. These are practical steps and actions that signatory organisations commit to taking and implementing to achieve GPAI model compliance.

Organisations are able to sign up to specific chapters, or the entire Code. Thus far, 26 organisations have signed up in full and xAI (Grok's creator) has signed up to the Safety and Security Chapter only. Meta announced that it will not sign up.

The Transparency Chapter focuses on the technical documentation which GPAI model providers are obliged to produce, maintain, and share with key stakeholders. It includes the 'Model Documentation Form' template, which providers can use to ensure they gather and document all the information which they are required to maintain and potentially share with the AI Office, national regulators, and downstream providers.

The Copyright Chapter focuses on how organisations can comply with the obligation to implement an EU copyright compliance policy. This includes measures for compliant web crawling and scraping and mitigating the risk of copyright-infringing outputs via technical guardrails.

Finally, the Safety and Security Chapter focuses exclusively on the obligations for providers of GPAI models with systemic risk. It consists of ten commitments, all relating to GPAI model risk identification, management, mitigation, treatment, monitoring,

ownership, and accountability.

The European Commission strongly encourages providers to sign the Code of Practice, noting its various benefits and calling it a "*straightforward way of demonstrating compliance*". The Commission even indicates that it will be more trusting of signatory organisations, due to their transparent approach.

It noted that providers who do not sign up may be "*subject to a larger number of requests for information and requests for access to conduct model evaluations throughout the entire model lifecycle because the AI Office will have less of an understanding of how they are ensuring compliance with their obligations*".

In future, the GPAI Code of Practice may be superseded by harmonised technical standards. These remain under development.

How and when will the GPAI model provisions be enforced?

The most important thing to understand is that the obligations relating to providers of GPAI models are enforced by the European Commission's AI Office, not member state regulators. This is in contrast to the rest of the AI Act's provisions.

With respect to enforcement actions, the AI Office has the following powers:

- Request information from providers.
- Conduct evaluations of GPAI models.
- Request the implementation of measures and mitigations.
- Recall GPAI models from the market.
- Impose financial penalties of up to 3% of global annual turnover or €15m (whichever is higher).

Because the AI Office is charged with enforcement, the European Commission's guidelines on GPAI models carry significant weight, even though they are not legally binding. In those guidelines, the Commission explained that it expects to forge close working relationships with GPAI model providers.

It encourages "*close informal cooperation with providers during the training of their GPAI models*", as well as "*proactive reporting by providers of GPAI models with systemic risk*". Given the various notification, reporting, and transparency obligations, there will be a lot of back and forth between providers and the AI Office.

For those that signed the Code of Practice, the AI Office's focus will be on monitoring their adherence to its measures. Expect slightly more leniency and goodwill. For those that opted not to, the focus will be on in-depth assessments and investigations as to how they are nonetheless compliant.

In terms of timelines for compliance and enforcement, the obligations for providers of GPAI models became applicable on 2 August 2025. This means that organisations are legally obliged to be compliant today. However, this is only for GPAI models that were placed on the market from 2 August 2025 onwards. As discussed above, for 'legacy' GPAI models placed on the market before then (i.e., the vast majority of GPAI models available today), providers have until 2 August 2027 to comply.

Although the obligations have been applicable since 2 August 2025, the European Commission, including its AI Office, does not have any enforcement powers until **2 August 2026**. This means there will be no enforcement proceedings or fines for at least one year from now. However, this does not change the fact that organisations are obliged to work on compliance from today. Any critical gaps in the first year may be taken into account in future enforcement actions or rulings.

Irrespective of the provision, and whether or not enforcement is managed by the AI Office or member state regulators, the Court of Justice of the European Union (CJEU) always has the final say on AI Act interpretation. Over the years, it will be interesting to monitor and learn from the inevitable GPAI model case law that will pile up.

Thanks for reading Enterprise AI Governance!
Subscribe for free to receive new posts and
support my work.