A&O SHEARMAN

INSIGHT

AI and accountability – Navigating responsibilities across the AI value chain

Accountability is a pervasive AI principle. But how to put it into practice?

READ TIME

7 mins

PUBLISHED DATE

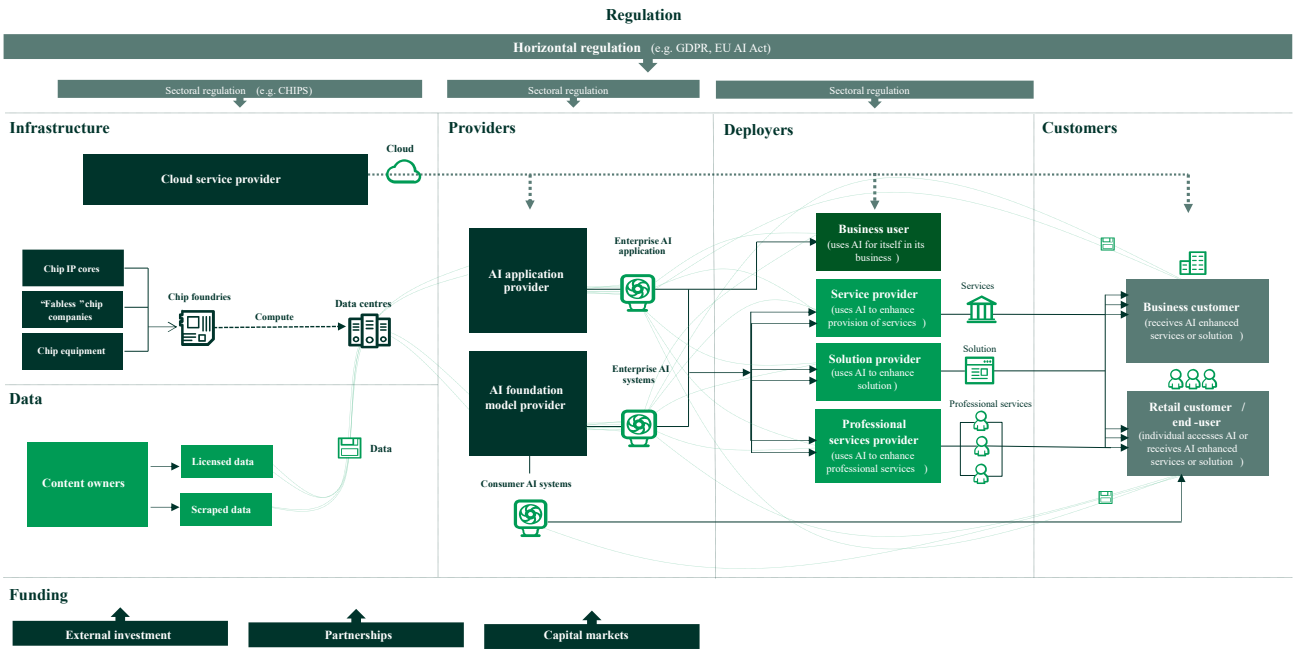
Feb 26 2025

Accountability is a pervasive AI principle. But how to put it into practice? If you're reading this note, you likely already know three things: the technology is evolving quickly; the regulation is evolving quickly and without consensus; complications and nuance abound, often to a dizzying degree.

Rather than talk about how complicated it all is, we want to try and bring some welcome clarity by laying out the key questions and

challenges companies will need to consider when building or deploying AI.

Below is the AI value chain. What 'accountability' means across this chain varies, depending on the AI system itself (the learning models underpinning it, the different actors involved in training it, the range of data sources etc), the role of the accountable person (which itself may not be static), the jurisdictions involved, and the interfaces between different stages of the value chain. Delivering accountability on an enterprise basis will require agility, co-ordination, and a sustainable approach to governance that can evolve over time.



To see this play out in practice, take the (common) scenario where a business is incorporating a third-party foundation AI model into a wider system or product, which it then commercializes.

Among other things, that business would need to consider:

What is your role? Do your AI activities bring you within scope of particular regulatory requirements or change your relationships with other entities in the value chain?

Your commercial intentions, place in the value chain, and technical solution will largely dictate your role and accountability approach. The way in which you use the third party AI model will have a bearing on expectations of customers and regulators. Are you taking the AI model and simply applying your own user interface before putting it on the market? Are you fine-tuning or using RAG enhancement to develop the model itself, too?

Any customisation activities will change your relationship with the underlying model and data used to train / customise it, and may also trigger a change in role categorisation under the EU AI Act. By making a substantial modification to a high-risk AI system or repurposing an AI system to create a high-risk system, a deployer may become categorised as a provider, with an important increase in regulatory obligations, and there is uncertainty as to what 'substantial' means for this purpose. This is as much a technical question as a legal one, which again highlights the need for co-operation and co-ordination across teams.

Similarly, there is uncertainty as to the nature and extent of any fine-tuning of a third party general purpose AI model would be sufficient to make you a 'provider' of that general purpose AI model for EU AI Act purposes. To ensure accountability, clarity on scope of obligations (both under regulation and under upstream and downstream contracts) is essential.

What do your contracts say? Do they address the 'squeezed middle'?

Drafting teams need a detailed understanding of the specific model types, data sources and use case design, as well as the relationships up and down the value chain, to advise pragmatically on risk allocation under contract.

Where you are building on top of a third-party AI model, you will be in the "squeezed middle", between risk allocation and requirements upstream, and downstream demands from your customers. For instance, depending on the use case, customers may adopt robust positions on IP infringement risk allocation, privacy compliance and data usage restrictions, and you may not be able to flow equivalent positions to the upstream AI model provider or obtain sufficient information and support to address customer and regulatory demands. Again, this is a technical question as much as a legal one. Some questions to ask that can help bring clarity:

- From a compliance perspective, are your contracts appropriately flexible to enable ongoing regulatory compliance despite the changing landscape?
- Do both your downstream and upstream agreements adequately address your regulatory and commercial requirements to align with your role? Provisions addressing compliance with law and associated assistance requirements are heavily negotiated in AIaaS agreements, often with prescriptive obligations imposed on developers to enable deployers to meet their own regulatory requirements (e.g. regarding transparency).
- Do your contracts address customer protections regarding conflicts of interest and benchmarking of alternative models? You and your downstream customers will be keen to make the most of the latest technology and ensure that the foundation model used is the best for the job. Vendor lock-in and third-party risk is a particular concern for many deployers who are increasingly aware that application developers may have potential conflicts of interest. They may, for example, favour using foundation models in which they have a commercial interest, even thought they might not be the best model for the particular use case.

Open source AI–why does it matter?

Much is made of AI models being "open" not least because open foundation models that do provide significant information on parameters may be able to take advantage of various regulatory derogations under the EU AI Act (unlike the GDPR), such as exceptions to certain transparency requirements.

If you're using an "open source" third party foundation model, you need to understand the extent to which it really is "open source". There is a spectrum of 'openness' among open models depending on what materials (i.e. model weights, code, data) are made available and on what terms. When building on top of open models, have you critically considered whether relevant license terms include acceptable use restrictions that may impair your or your customers' usage of the model (or its outputs), or any liability provisions that may affect the flow of accountability between you and "open source" provider?

How can AI governance address fragmented and uncertain regulatory risks across relevant elements of your AI lifecycle?

AI governance is ultimately change management, and there are few parts of an organization that are untouched by it. Wide stakeholder collaboration is key to understand the risk landscape and available mitigants, both of which will span many different parts of an organization (from front office business / product teams to risk control functions, infosec and technology offices). The evolving nature of AI and the importance of governance in this context is driving the development of new AI governance regimes within organizations.

Businesses are trying to regulate within their walls just as nation-states are, and all face the same tricky balancing act: centralized oversight versus driving adoption and innovation. Again, asking the right questions is the first step in bringing much-needed clarity.

- Have you considered the right balance of centralized oversight of AI use cases with fostering innovation and driving adoption?

- Does your governance approach address the whole AI lifecycle and interaction with external stakeholders (not least the model provider)?
- Have you considered adopting an industry standard when developing AI, e.g. NIST?
- Do outputs from risk and impact assessments, due diligence and reviews link to tangible defined risk mitigations?
- Does the governance structure clearly allocate responsibilities to enable effective accountability?
- Crucially, is your governance approach flexible and capable of adapting as technological and regulatory requirements change?
- Have you looked at AI-specific regulation in the wider landscape of data and digital governance? Accountability is a concept that stretches beyond AI specific requirements and the true AI regulatory landscape encompasses the likes of data protection and privacy, IP, cybersecurity, antitrust, and sector-specific laws. To a greater or lesser degree, liability can arise under any one or more of these regimes depending on the specific scenario. For instance, if you will use a general purpose AI system to generate software, there are specific IP risks that arise from AI for coding and these will be more important to you and your customers than the privacy / bias / transparency requirements that may arise on, say, customer-facing chatbots. How do you integrate your regulatory compliance approach to ensure you address all areas of risk? Can you leverage any existing processes and procedures to fulfil your new AI accountability needs?

Keeping pace

Codes and guidance on the EU AI Act will invariably contain wording that can be pointed to in any accountability documentation. We have seen the EU Commission park the proposed AI Liability Directive - what comes next? AI insurance products are developing - will they function as a backstop for liability - can they help close commercial gaps? How will the geopolitical landscape

impact regulatory emphasis? How will your business needs drive evolution of internal risk appetite? Continued, proactive engagement is key to making the most of AI opportunities without falling foul of regulatory risk.

Related capabilities

Artificial intelligence Technology