The role of the GDPR in regulating AI:

Less **'big brother'**, more **'big mother'**

Jade Kowalski
Partner
T: +44 (0) 20 7894 6744
jkowalski@dacbeachcroft.com

Charlotte Halford
Partner
T: +44 (0) 20 7894 6492
chalford@dacbeachcroft.com

In the past two years, AI has surged from a technical curiosity to a boardroom imperative. There is little doubt that AI will remain the topic of interest to businesses, regulators and data protection practitioners in 2025. As organisations continue workstreams that attempt to balance the maximising of opportunities with risk management, the pace at which external legal and regulatory factors must be considered is expanding rapidly.

A flurry of activity in the EU, UK and beyond

Of course, existing legal liabilities arising from the use of AI systems are already extensive – from data protection to intellectual property and from breach of contract to negligence.

However, when it comes to AI specific legislation and regulation, governments worldwide have been grappling with tough questions. Can this be achieved by existing frameworks or is dedicated AI legislation necessary? How to strike the right balance between fostering innovation and effective regulation? Are sector-specific rules required?

Unsurprisingly, no universal approach has emerged. Different jurisdictions are charting distinct paths, reflecting local priorities, philosophies about technology and broader culture.

In the EU, the AI Act entered into force on 1 August 2024. Despite being many years in the making, the final stages of negotiations were tense, with some concern that the draft may fall at the final hurdle. As we know, that did not happen due to a number of different factors, a key one being the desire to maintain the 'Brussels effect' – the ability of EU regulation to influence global standards and policies in circumstances where a number of jurisdictions were in the midst of considering their own approach to AI policy.

On passing the EU AI Act, Dragoş Tudorache, the LIBE rapporteur, stated:

> *"We delivered, the EU delivered. No ifs, no buts, no later. These are the rules we have forever attached to the concept of artificial intelligence, the fundamental values that form the basis of our societies. And with that alone, the act has nudged the future of AI in a human-centric direction, in a direction where humans are in control of the technology and where it – the technology – helps us leverage new discoveries, economic growth, societal progress, and unlock human potential… We need to put our entire diplomatic and political clout in promoting the European model of AI governance. This is a strategic priority for the next mandate, alongside reducing our strategic dependencies and increasing our resilience – because the future is AI-fuelled and we must continue to shape it."*

Activity to prepare for the EU AI Act is set to intensify further as its provisions phase in, starting with those prohibiting the use of 'unacceptable risk AI' from 1 February 2025.

In the UK, the journey towards AI regulation is moving at a slower pace. Depending on your perspective, this could be viewed as promoting innovation or generating uncertainty. The approach of the previous government was explicitly stated to be 'pro-innovation', such term being the title of a White Paper which proposed regulation by reference to 'AI principles', enforced by existing regulators on a sector specific basis.

Following the election of a Labour Government in 2024, there has been a change in approach and a proposal for specific, targeted legislation is now expected imminently.

Looking West, the United States, often regarded as a global tech leader, has tackled AI regulation through Presidential Executive Orders and various state and federal measures. However, these approaches are fluid, and depending on political leadership, potentially subject to change, particularly in light of the change in presidency of the United States. In Canada, the draft proposed Artificial Intelligence and Data Act would legislate for the responsible design, development and deployment of AI system, although its passage through the legislative process remains slow.

Looking from the Americas across the Pacific, Japan currently relies on existing laws and government guidelines to regulate AI systems, but a 2024 White Paper suggested that *"Japan should aim to become the 'world's most AI-friendly country'… with the best understanding of AI and the easiest implementation of AI in the world."* In China, the "Interim Measures for the Management of Generative Artificial Intelligence Services" were implemented in 2023, which supplement a number of existing laws, and a wider reaching Artificial Intelligence Law is currently in draft format.

Supervisory authorities: interim guardians

While governments and legislatures across the world continue to grapple with the complexities of AI regulation and policy approach, technological developments have continued to evolve. In the face of ongoing developments and often in lieu of a dedicated regulatory regime, data protection regulators have been quietly (and, in some instances, not so quietly) establishing themselves as the 'interim guardians' on AI risk, utilising the existing guardrails provided by data protection law.

Early on in the acceleration of generative AI, the Italian supervisory authority (the Garante) set the tone by commencing an investigation against Open AI, resulting in a temporary ban on ChatGPT in Italy in early 2023. The ban was subsequently lifted once OpenAI addressed concerns around the lawful basis for collection and processing of personal data used to train ChatGPT. In December 2024, the investigation concluded with the announcement of a EUR15 million fine in respect of violations relating to transparency and lawful bases.

The French, Spanish and German authorities had followed the Italian authority with their own investigations into Open AI, which (at the time) did not have European headquarters established (now located in Ireland) and therefore no lead supervisory authority. The Irish Data Protection Commission (DPC), will now continue investigations into any EU GDPR violations of an ongoing nature. There are a number of other examples including the delayed launch of Google Bard, and fines imposed on Deliveroo in Italy (for the use of AI technology to automatically rate rider performance) and Clearview AI in France (in respect of web scraping for the purposes of facial recognition technology).

In the UK, action from the Information Commissioner's Office (ICO) has chosen to focus on the process of developing AI systems, issuing a preliminary enforcement notice to Snap, Inc. In this matter, the ICO considered that the Data Protection Impact Assessment carried out in advance of the launch of Snap's AI chatbot was inadequate. In fact, it required that Snap reassess its efforts no less than five times, until the ICO was satisfied that the assessment was adequate. At the time, Stephen Almond (Executive Director of Regulatory Risk) stated:

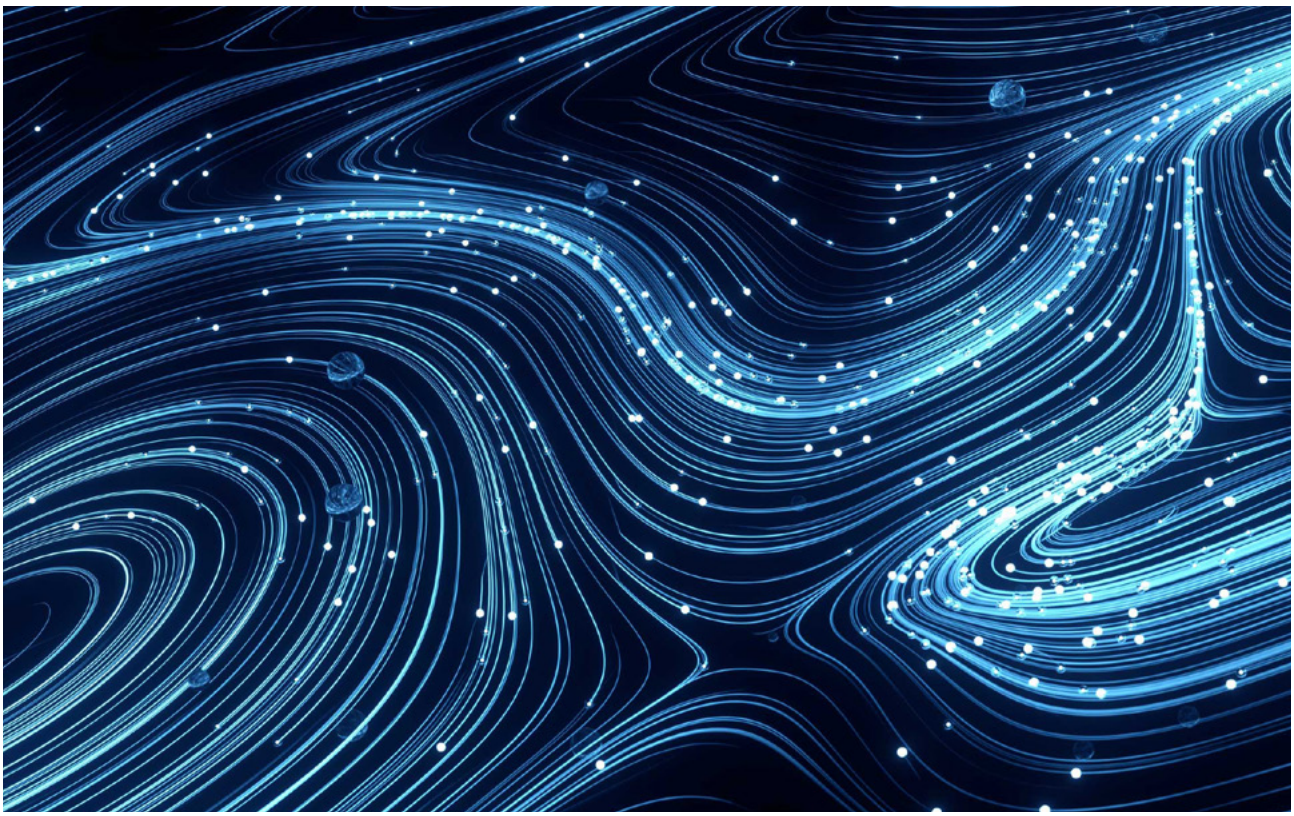
> *"Our investigation into 'My AI' should act as a warning shot for industry. Organisations developing or using generative AI must consider data protection from the outset… We will continue to monitor organisations' risk assessments and use the full range of our enforcement powers – including fines – to protect the public from harm."*

What is particularly interesting is that supervisory authorities are choosing to utilise tools other than financial penalties. Arguably, such alternative measures are more effective than fines, the size of which usually pale into insignificance when considered against the deep pockets of big tech companies. However, a ban on the use or launch of a new product can cost organisations their competitive advantage, which will often constitute a far greater cost.

As a result of these enforcement activities, there has been much discussion regarding the formal role of the data protection authorities.

Indeed, in July 2024, on the same day that the final text of the EU AI Act was published in the Official Journal, we saw guidance from the CNIL in France, a clear indication that the regulator sees itself taking a key role. The European Data Protection Board (EDPB) has gone so far as to recommend that EU supervisory authorities be designated as 'market surveillance authorities' (being the national competent authority for the purposes of investigating infringements and carrying out enforcement in respect of breaches of the EU AI Act), emphasising:

> *"the experience and expertise gathered by [the DPAs] in working out guidelines and best practices and carrying out enforcement actions on AI-related issues with respect to the processing of personal data at both national and international level. DPAs have proven and are proving to be indispensable actors in the chain leading to the safe, rights-oriented and secure deployment of AI systems across several sectors".*



GDPR: The elder stateswoman

What of the fate of the GDPR as specific AI legislation and regulation evolves? Of course, the GDPR will continue to be the primary instrument for data protection obligations and enforcement. It's role as complimenting the EU AI Act has already been acknowledged.

The CNIL emphasised this synergy, stating that *"the AI Act does not replace the requirements of GDPR…* [instead]*, it aims to complement them by laying down the conditions required to develop and deploy trusted AI systems."* The EDPB echoed this perspective, describing the AI Act and EU data protection legislation as *"complementary and mutually reinforcing instruments".* The ICO also reiterated that existing data protection laws are 'technology-neutral' and *"adaptable* [and therefore being] *able to respond to new technologies, including advances in AI."*

However, we suggest that the GDPR has an even more important role to play as it takes on the role of 'elder stateswoman', providing a rich library of guidance, enforcement and case law to support the interpretation of similar obligations and concepts under the EU AI Act and other AI specific legislation.

By way of examples, authorities in a number of Member States including France, Spain and Germany have produced guidance on the application of concepts such as transparency and data minimisation with direct read across to principles under the EU AI Act. In the UK, the joint guidance produced by the ICO and The Alan Turing Institute provides a useful basis when considering how to comply with obligations arising from the 'right to explanation of individual decision making' under Article 86 of the EU AI Act.

Innovation with a side of caution or confusion?

However, even with the reliability of well-established law, regulators and guidance, the landscape is not simple. As the privacy challenges continue to crystalise and regulatory scrutiny intensifies, supervisory authorities are keen to emphasise that current data protection frameworks are not intended to hinder and stifle innovation. The key message communicated is the need to strike a balance between fostering technological advancements and safeguarding fundamental rights.

As observed by Lee Kupferman, co-founder of Phare Health, a provider of AI powered financial tools to hospitals:

"AI innovation is always going to be a step ahead of the laws. Strict regulations driven by a fear of the unknown are likely to stifle innovators - adaptive yet effective guidelines will strike that balance between personal privacy and encouraging businesses to leverage the latest tools."

However, a key obstacle to achieving that balance in practice is the divergence in approach, both between EU supervisory authorities themselves and the ICO and its EU counterparts (which we explore more fully in our associated piece in this collection). There is a risk that this divergence could stifle innovation, just as much as a lack of regulatory clarity.

To examine one example, the issue of data (or web) scraping has gained increasing global attention coinciding with the development of generative AI platforms. The ICO helpfully summarises this issue as follows:

> *"Most developers of generative AI rely on publicly accessible sources for their training data. Developers either collect training data directly through web scraping, indirectly from another organisation that has web-scraped data themselves, or by a mix of both approaches. In either approach, developers need to ensure the collection of the personal data they process to train models complies with data protection."*

The ICO, along with 16 other global data protection authorities (including some, but not all, EU Member States), has contributed to a recently concluded statement on data scraping and the protection of privacy, which emphasises that:

> *"publicly accessible personal data is generally subject to data protection and privacy laws and should be adequately protected against unlawful scraping,"*

noting that a failure to do so could result in regulatory intervention. The statement, however, did not propose a unified approach to the circumstances in which scraping may be considered permissible, leaving the issue to individual authorities (and back in the realms of uncertainty and potential divergence).

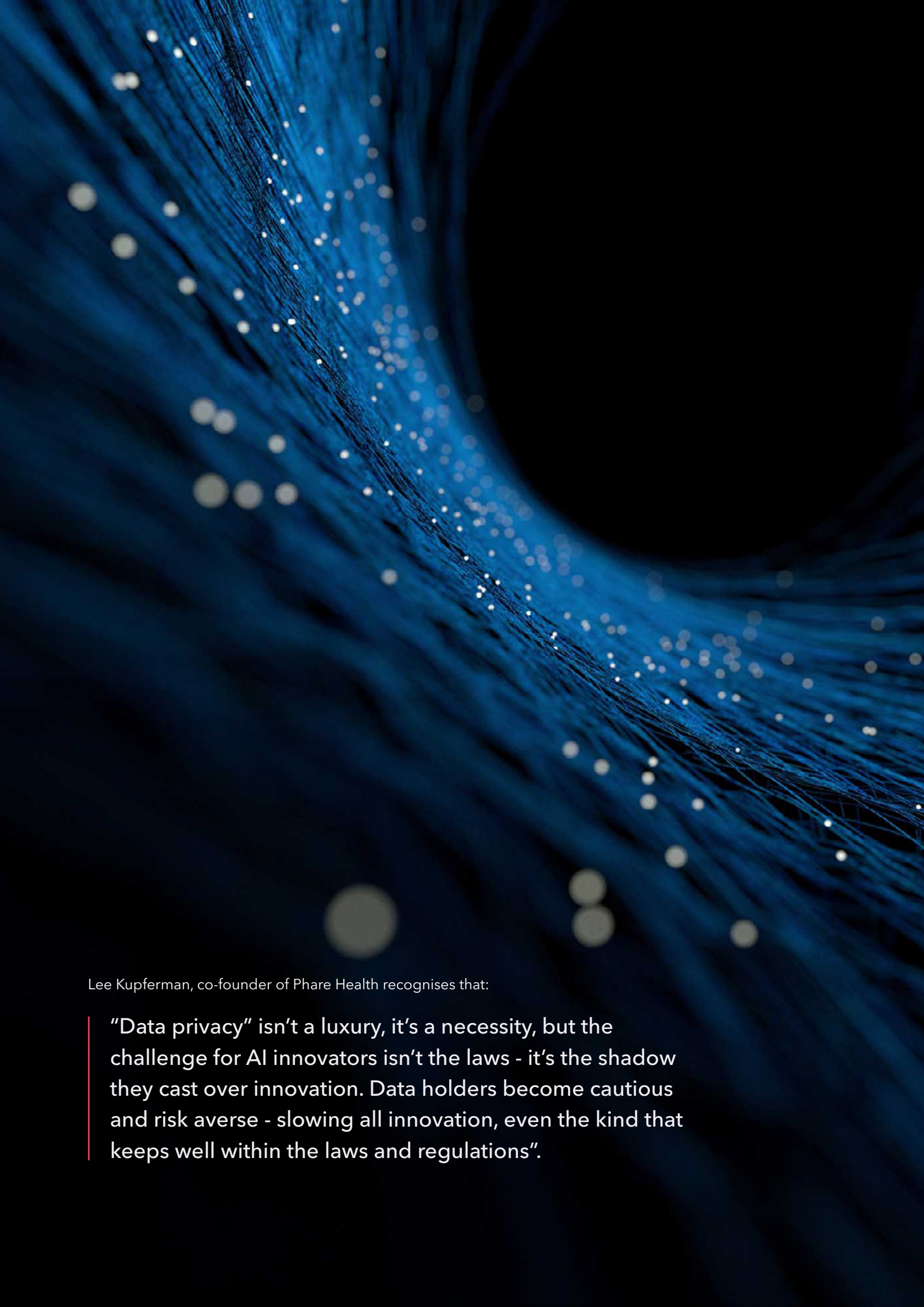
As part of its continuing work on AI, the ICO launched its own consultation series on the application of data protection law to generative AI in early 2024. The aim of the consultation was to move swiftly to *"address any risks and enable organisations and the public to reap the benefits of generative AI"*. The consultation explored five key areas, including the lawful basis for web scraping to train generative AI models. Publishing its response in December 2024, the ICO reiterated its initial view that legitimate interests is the only available lawful basis for using web-scraped data to train generative AI, requiring the passing of the three-part 'legitimate interest assessment' test. Considering the other lawful bases, the ICO expressed the view that consent would be unlikely to apply in this instance due to practical difficulties in ensuring that such consent meets the required standard.

Looking to the EU by way of comparison, the French CNIL published a focus sheet on web scraping whereby it agreed with the ICO's position, stating that the collection of *"data accessible online to create a training dataset may be based on the legitimate interest."* The Italian Garante has also issued guidance on the topic, although it noted that it was waiting to decide *"the outcome of a number of investigations already under way..."*

In contrast, the Dutch Data Protection Authority has taken a stricter view, asserting in its guidance that organisations cannot rely on the legitimate interests basis to justify the collection and processing of web scraped data. Instead, it recommends that explicit consent is required – a requirement that poses significant practical challenges (as identified by the ICO in the UK).

This lack of consensus and clarity has led several major tech companies to halt the training of their generative AI models. For example, Meta paused plans to use Facebook and Instagram user data to train its models following concerns about how users were able to object to such processing. Meta resumed plans in the UK in September relying on the 'legitimate interests' basis to process the data. However, it has yet to take similar steps in the EU, highlighting the disparity in regulatory clarity between regions.

This regulatory inconsistency has divided opinions. Technology companies criticise the assertive approach taken by some European regulators, arguing it stifles innovation and development. Meanwhile, privacy campaigners in the UK express frustration with what they see as the ICO's 'tolerant and permissive' approach. The Open Rights Group has referred to an 'AI enforcement gap', citing the decision of the same major tech companies to continue their plans to train AI models in the UK whilst halting similar efforts in the EU.



Lee Kupferman, co-founder of Phare Health recognises that:

> “Data privacy” isn’t a luxury, it’s a necessity, but the challenge for AI innovators isn’t the laws - it’s the shadow they cast over innovation. Data holders become cautious and risk averse - slowing all innovation, even the kind that keeps well within the laws and regulations”.

The EDPB will play a key role in seeking harmonisation where possible. In December 2024, it released Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. The Opinion considers a number of different topics including when and how an AI model can be considered anonymous and the use of 'legitimate interests' as a legal basis for developing or using AI models. The opinion also sets out views on general considerations such as accountability, transparency and purpose limitation. Specifically on web-scraping, the EDPB provides a non-exhaustive list of mitigating measures in relation to the development phase, including the provision of web scraping. However, the opinion emphasises that any mitigating measures:

> "*may be subject to rapid evolution and should be tailored to the circumstances of the case. Therefore, it remains for the supervisory authorities to assess the appropriateness of the mitigating measures implemented on a case-by-case basis.*"

The opinion was accompanied by a press release which expressly stated that the EDPB is *"currently developing guidelines covering more specific questions, such as web scraping."*

Evolving the Existing Toolkit

As regulators navigate unchartered waters in the AI era, how is the existing data protection and privacy framework rising to the challenge? What measures are keeping the system afloat? What tool has been the unsung hero of this effort?

Recent developments have promoted the data protection impact assessment (DPIA) as a vital instrument in addressing AI's privacy challenges. The ICO identifies DPIAs as 'effective roadmaps' to support organisations identify and mitigate risks to individuals' rights and freedoms. A well-conducted DPIA is key to managing these risks effectively. Although not all AI use cases will fall within the mandatory requirement for a DPIA, a large number will and, in any event, most organisations will be keen to carry out an enhanced privacy assessment of new AI initiatives.

How important is it to get a DPIA right? The aforementioned ICO investigation in relation to Snap's AI chatbot provides important learnings and the Decision is a must-read for those completing DPIAs. It provides key takeaways on the content and level of detail expected from the ICO which can be utilised in practice.

Similarly, in another high-profile matter, the Irish Data Protection Commission (DPC) recently commenced a cross-border inquiry into Google's compliance with DPIA requirements. The investigation focusses on the processes followed by Google during the development of PaLM2, its foundational AI model. The DPC press release underscored the *"crucial importance"* of the DPIA in *"ensuring that the fundamental rights and freedoms of individuals are adequately considered and protected."*

These matters serve as a reminder that DPIAs are not merely procedural—they are integral to demonstrating accountability in the development and deployment of AI systems. We expect the focus on both the process and content of DPIAs to continue to serve as a cornerstone of regulatory oversight.

GDPR as 'big mother'

As we enter 2025, the GDPR is taking on a new role; that of the 'big mother' of AI regulation. It's core principles – accountability, transparency and fairness – have proven adaptable to emerging technologies. While the regulatory framework may evolve over time, the GDPR's foundation remains robust, capable of guiding organisations through the complex and ever-changing AI landscape.

Full list of references available upon request