



AI in Europe: Road Map for Navigating the IP, Data Protection and Regulatory Considerations

This article was published in the **September 2023 issue of *Insights***.

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Eve-Christie Vermynck

Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Alistair Ho

Associate / London
44.20.7519.7005
alistair.ho@skadden.com

Jonathan Stephenson

Associate / London
44.20.7519.7038
jonathan.stephenson@skadden.com

Key Points

- Organizations developing or using generative AI tools should implement cross-functional governance frameworks to develop and continuously monitor their use of such tools.
- From the earliest stages of generative AI use, organizations should assess the data protection, cybersecurity and intellectual property risks, particularly in relation to any training data used by the generative AI tool.
- European regulators are actively considering the implications of generative AI. A new EU law governing AI that takes effect in the spring of 2024 will classify AI systems and impose appropriate associated safeguards, including for transparency.

The 25.5% compound annual growth in the artificial intelligence (AI) market in Europe, coupled with the anticipated increase in European spending on AI tools — from \$33.2 billion currently to over \$70 billion by 2026 — has left many organizations considering how best to engage with AI in Europe.¹

In this article, we take a closer look at emerging regulatory frameworks for generative AI as well as how organizations interested in developing or using generative AI tools can best align with existing regulations to mitigate risks related to data privacy, cybersecurity and intellectual property (IP).

What Organizations Should Consider

This article focuses on generative AI tools — tools such as ChatGPT that take input prompts and produce output that imitates human intelligence. These have attracted the most regulatory concern in Europe.

¹ International Data Corporation (IDC) *Worldwide Artificial Intelligence Spending Guide* (V1 2023).

AI in Europe: Road Map for Navigating the IP, Data Protection and Regulatory Considerations

When discussing generative AI tools, there are broadly speaking three stages to consider: the **inputs** that are fed into generative AI tools (user prompts and training data), the tool itself and the **outputs**. (See our Spring 2023 *The Informed Board* article “[What Is Generative AI and How Does It Work?](#)”)

From the standpoint of organizational responses, governance is central at each stage. Due to its transversal nature, organizations should identify and connect the relevant stakeholders involved in the development, deployment and use of a generative AI tool, such as commercial, legal, compliance, data protection and cybersecurity, and information technology teams. Generative AI requires a cross-functional governance structure balancing stakeholder inputs and direct board-level reporting, particularly given the emerging regulatory framework detailed below.

Organizations should consider:

- Framing and designing the intended application of generative AI with a documented AI impact assessment.
- Proactively implementing training, safeguards, logs and accountability measures to manage internal behaviors.
- Regularly monitoring implementation gaps and remedying them from time to time.

Emerging Regulatory Framework

AI-specific regulation. In light of the rapid pace of AI development, there is a clear appetite among regulators to establish AI-specific rules, as evidenced by the June 2023 [joint release by the G-7 data protection authorities](#) that highlighted that collaboration among them would be necessary.

The European Union is leading the way with the EU Artificial Intelligence Act (AI Act). Scheduled to take effect in the spring of 2024, this will be the first comprehensive law on the use, deployment and development of AI. Although there is a grace period (likely two years from implementation), the AI Act’s extraterritorial effect and anticipated administrative fines of up to €30 million or 6% of annual global revenue, whichever is greater, have placed AI firmly on organizations’ radars.

There are still key points to be negotiated (in particular, the definition of AI), but the draft rules establish a consumer protection-driven approach through a risk-based classification of AI systems.

In parallel, the EU is amending its product liability regime with the revised Product Liability Directive and the AI Liability Directive, with an aim toward providing certainty and recourse

to consumers in relation to defective or harmful AI products. Additionally, the Network and Information Security Directive (NIS2) and the proposed EU Cyber Resilience Act will complement the AI Act by providing a set of cybersecurity standards for high-risk AI tools.

Meanwhile, the U.K. is taking an incremental sector-led approach to AI regulation, as reflected in its June 2023 [white paper](#). The U.K. government is expected to share high-level guidance and an initial regulatory road map in the coming months with regulators, who will in turn share tailored recommendations in the financial, health care, competition and employment areas. The U.K. government will then assess whether AI regulation or an AI regulator is required.

Competition. European competition authorities are considering whether AI will reduce competitive pressure, facilitate collusion and lead to abuse of a dominant position. For example, the U.K.’s Competition and Markets Authority recently carried out an initial review to assess the potential implications of AI foundation models and how their use will develop. Additionally, the EU Digital Markets Act (DMA) may regulate AI to the extent that a “core platform service” (e.g., cloud computing, online search engines and virtual assistants) includes AI tools.

Foreign direct investment (FDI). With AI’s clear potential implications for national security, foreign investment screening regimes across Europe generally deem AI to be a sensitive sector, triggering mandatory approval requirements for foreign investors. Since many FDI screening regimes have no or very low de minimis thresholds, even early-stage ventures may find foreign investors unable to invest without government approval.

Financial services. Currently, there is no European regulation that specifically governs the use of AI in financial services. However, the U.K. Financial Conduct Authority and Prudential Regulation Authority published a [discussion paper](#) in November 2022 on the potential risks and benefits of AI, which noted that certain existing rules will apply to AI in financial services.

How Does Generative AI Fit Into Existing Data Protection and Cybersecurity Frameworks?

Documenting the Data and the Process

The creation and ongoing use of any generative AI tool requires large data sets that the machine learning model uses to “learn” and improve its output. These data sets, which could include personal data, may be purchased from third parties under a data sharing agreement, extracted from the internet via web scrapping or inputted by users via prompts.

AI in Europe: Road Map for Navigating the IP, Data Protection and Regulatory Considerations

Organizations should take a structured approach to managing compliance with European data protection laws, including the General Data Protection Regulation (GDPR), by mapping data flows and documenting the data sources, types of personal data, purpose and lawful basis for processing, and the form in which it is processed and stored (e.g., aggregated, pseudonymized, encrypted, synthesized).

For example, under the GDPR, a generative AI tool owner acting as controller may be able to rely on its legitimate interest to lawfully undertake data processing activities, which will be balanced against individuals' rights and freedoms and documented by way of a legitimate interests assessment updated from time to time. Where "special category data" (e.g., race, ethnicity, genetic, biometric, health data) is processed, the controller will likely need the data subject's explicit consent in order to process that data lawfully.

Where the generative AI system is used for automated profiling or decision-making, additional safeguards should be put in place to prevent bias or discrimination, including introducing human inputs and oversight.

Implementing Safeguards

From the formative stages of generative AI use, organizations should work with the principle of "privacy by design" in mind, often documented in regularly updated risk or data protection impact assessments. Having appropriate technical and organizational measures to safeguard the personal data involved in any generative AI tool (e.g., masking, encryption, anonymization, pseudonymization, privacy enhancing tools, contractual data processing agreements with third parties) is crucial.

Maintaining Transparency With Users

European data protection laws require that information be given to individuals about the processing of their personal data in clear and easily accessible language, in a privacy notice provided before the data is processed. Mapping data flows will help organizations create compliant privacy notices, in particular in relation to foundational models where the AI rules may not be easily understood by individuals whose data is being used.

Generative AI controllers will also need to consider how to adequately address and respond to rights requests from data subjects (e.g., access, correction, deletion). European data protection authorities have made it clear that they will not interpret the exemptions to data subject rights request obligations more broadly in the context of AI.

How Does Generative AI Fit Into Existing Intellectual Property Rights Frameworks?

Mitigating the Risk of Infringement Claims at the Input Stage

As noted above, organizations often purchase third-party data sets and undertake web scraping to create a large training data set. Organizations should assess the training data they are receiving so that they can determine the nature of intellectual property rights (IPRs) subsisting therein, including the scope of usage rights granted by way of licensing agreements. This will require assessment of both registered (patents) and unregistered (copyright, know-how, trade secrets) IPRs and the IPR-related agreements.

In order to ensure that the generative AI tool will operate in compliance with IP-specific contractual rights and restrictions, organizations should be aware of fields of use, territorial restrictions, sublicensing rights, ownership of any modifications or improvements, financial conditions, and grounds and consequences of termination. As some of the players in the AI space are relatively new, organizations could also benefit from considering the third-party content provider's IP profile, *i.e.*, whether they have been involved in infringement or invalidity proceedings, how they safeguard their IP and data and whether they solely or jointly own the IP.

The incorporation of open source software (OSS) should be closely monitored. The OSS license may include restrictions that could affect the use of the generative AI tool and output, or even in some cases require the release of any OSS-related modifications to the community at large.

Though web scraping is common in compiling datasets for training AI models, organizations should closely consider whether that is necessary because web scraping may infringe third-party IPRs. (The EU did introduce some exceptions in the Digital Single Market Directive for scientific research, publicly available and licensed data).

IP Protection for Generative AI Output

It remains to be seen whether the outputs of generative AI tools can enjoy IP protection. For example, for copyright to apply in the Europe, the work must be an original intellectual creation from one or more authors. Work created by generative AI tools generally don't fit this requirement, as the tools may produce either outputs that are substantially similar to portions of training data or very similar outputs for various users (depending on the generality of the user prompt), meaning that the output may not be original.

AI in Europe: Road Map for Navigating the IP, Data Protection and Regulatory Considerations

With regard to authorship, in the case of an AI-generated work, the author may be a generative AI tool itself, and the prompt given to the tool may have been developed jointly, by a number of people in different shares or solely by the generative AI tool, which is entitled to no protection. (See our August 28, 2023, client alert [“District Court Affirms Human Authorship Requirement for the Copyrightability of Autonomously Generated AI Works”](#) for

how U.S. law is approaching this issue.) Whether the courts and legislature will seek to develop the rules around IP treatment of AI-generated work as the industry continues to grow is an open question.

Counsel **Jason Hewitt**, associate **David Y. Wang** and professional support lawyer **Elizabeth Malik** contributed to this article.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West / New York, NY / 10001 / 212.735.3000

22 Bishopsgate / London / 44.20.7519.7000