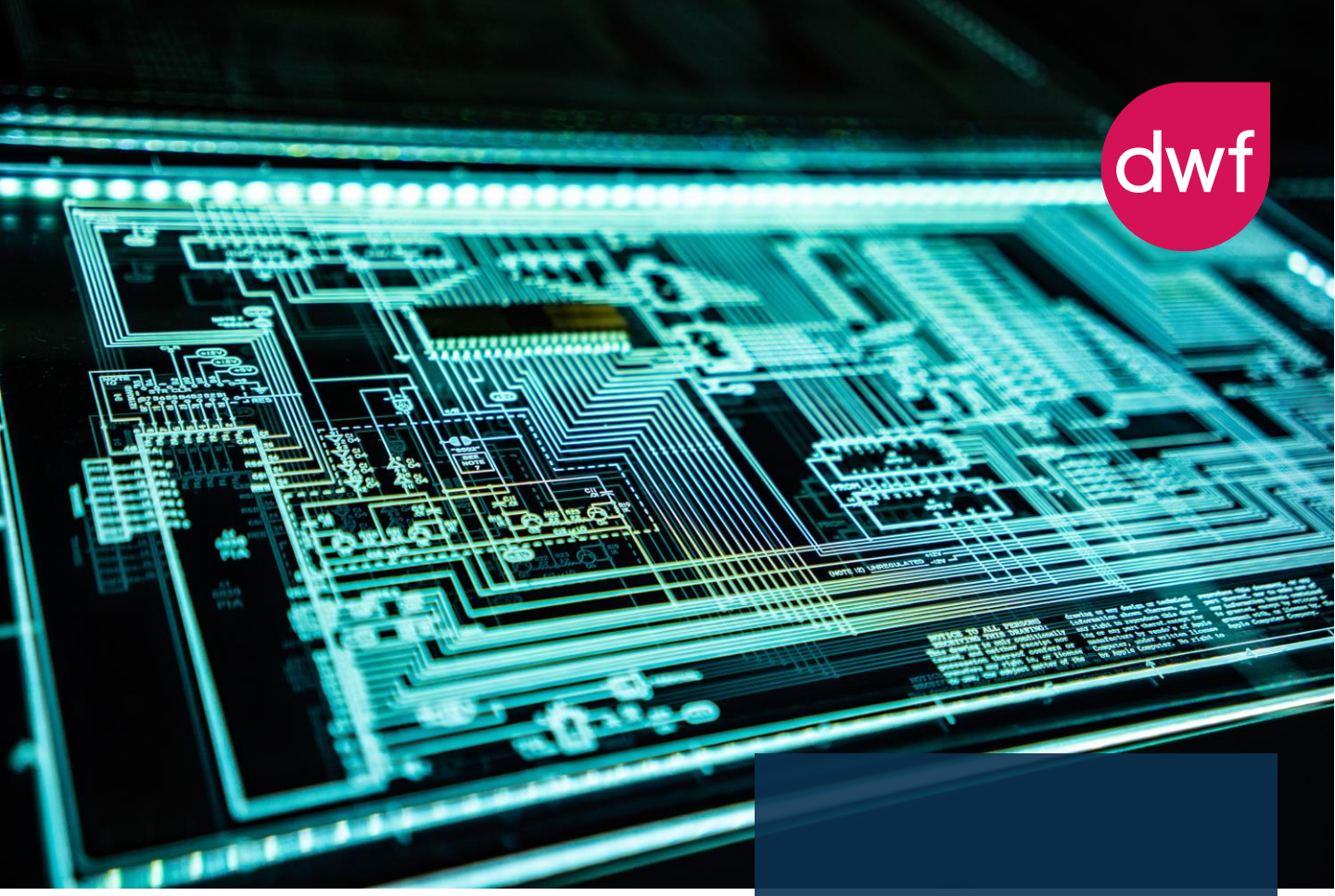


Newsletter

Tech / Data

September - October 2025

Data Privacy Framework approved by the EU

The European Union confirms the validity of the Data Privacy Framework, ensuring legal certainty for data transfers to the United States (for the time being)

In this issue

In this issue

LATEST NEWS - TECHNOLOGIES

Study on the interaction between the AI Act and the European Union digital legislative framework by the European Parliament

European Parliament, Interplay between the AI Act and the EU digital legislative framework, 30 October 2025

European Parliament, Interplay between the AI Act and the EU digital legislative framework, 30 October 2025, At a glance

A study by the European Parliament analyses the interactions between the AI Act and the main texts of the European Union's digital legislative framework, including the GDPR, DSA, DMA, CRA and NIS2 Directive. Although each regulation pursues a legitimate objective, their combination raises concerns about the consistency, competitiveness and innovation capacity of the European AI sector. The dense and layered regulatory framework creates overlaps, gaps and legal uncertainties.

Among the tensions identified, the AI Act extends product safety logic to complex areas such as fundamental rights, which are difficult to assess with traditional compliance tools. It applies to both suppliers and users of AI systems, creating complex chains of responsibility that are particularly burdensome for SMEs. High-risk systems are defined by annexed lists and subjective criteria, introducing legal ambiguity. Despite the existence of regulatory sandboxes and exemptions for open-source software, the framework remains focused on risk management, to the detriment of innovation. Furthermore, the new AI office, responsible for supervising GPAIs and coordinating enforcement, encroaches on the powers of established authorities.

There are numerous points of friction with other legislation: the GDPR imposes redundant impact assessments and overlapping transparency obligations; the CRA and NIS2 introduce similar obligations in cybersecurity; the DSA and DMA impose sometimes contradictory transparency and accountability rules for AI-generated content.

The study recommends, in the short term, promoting common guidelines and mutual recognition of assessments; in the medium term, clarifying roles and simplifying obligations; and in the long term, building a coherent European digital framework that is conducive to innovation while ensuring the protection of fundamental rights.

LATEST NEWS - TECHNOLOGIES

Charter of the Paris Economic Activities Tribunal to regulate the use of artificial intelligence systems

Paris Economic Activities Court, Charter on the use of artificial intelligence systems and personal and sensitive data within the Paris Economic Activities Court, 9 September 2025

On 9 September 2025, the Paris Economic Court adopted a charter to regulate the use of artificial intelligence (AI) in its judicial and administrative functions. The text aims to ensure the responsible, ethical and transparent use of AI in the judicial context.

The charter affirms that AI must remain a decision-making tool, not a substitute for human thought. It encourages an approach based on caution, moderation and responsibility. Judges are invited to use these technologies sparingly, only within the scope of their duties, and taking into account their environmental impact.

AI tools must be validated by the court, and magistrates are required to verify the accuracy of the responses generated. The protection of personal and sensitive data is central: judges must comply with privacy policies, secure the information of litigants and ensure transparency in the use of AI. Litigants must be informed when their rights are affected.

A control mechanism is in place: any anomalies must be reported to the digital committee, and judges must undergo training dedicated to AI and data protection. This charter embodies a desire to reconcile legal tradition and technological innovation by promoting modern, rigorous justice that respects fundamental rights in a constantly evolving digital environment.

CNIL sanction against La Samaritaine for hidden cameras in the store's stockrooms

CNIL, Decision of the restricted panel imposing a financial penalty on SAMARITAINE SAS, 18 September 2025, No. SAN-2025-008

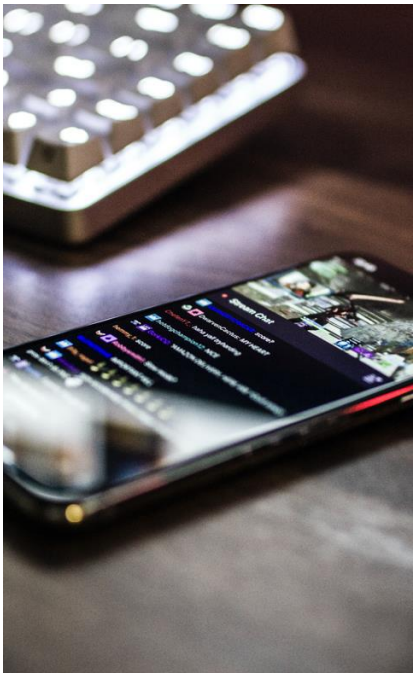
On 18 September 2025, the CNIL imposed a fine of €100,000 on SAMARITAINE SAS, which operates the store of the same name, for installing hidden cameras in the store's stockrooms. These devices, disguised as smoke detectors and equipped with microphones, were installed in August 2023 to combat a rise in thefts. Discovered by employees, they were removed in September 2023.

Alerted by a press article and a complaint, the CNIL carried out an inspection and found several breaches of the GDPR:

1. Breach of fairness and accountability: the cameras were concealed without prior compliance analysis or documentation of their temporary nature. They were not mentioned in the processing register or in an impact assessment, and the data protection officer had not been informed.
2. Excessive data collection: the microphones recorded personal conversations between employees, which constitutes a violation of the principle of data minimisation.
3. Failure to involve the DPO: the data protection officer was only informed after the installation, when she could have advised on the risks and measures to be taken.

The CNIL points out that the use of hidden cameras may be permitted in exceptional circumstances, provided that a fair balance is struck between security and privacy, which was not the case here.

LATEST NEWS - TECHNOLOGIES



Transparency of AI-generated content: labelling comes into force in China

Regulations on the management of deep synthesis of Internet information services, 11 December 2022

In accordance with the AI regulations adopted in 2022, China has imposed mandatory labelling since the 1st of September 2025 for all content generated or modified by artificial intelligence, whether text, image, sound, video or music. This obligation stems from the Measures for the Administration of Deep Synthesis Internet Information Services.

The system is based on dual labelling:

- a visible indication for the user,
- a digital watermark or metadata ensuring traceability.

No exceptions are provided for, either for art or satire: transparency is established as an absolute principle of digital fairness.

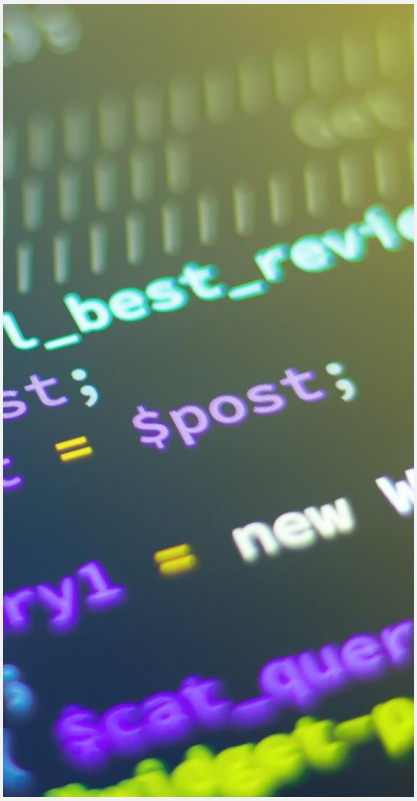
Class action lawsuit in the US against Apple over the training of its artificial intelligence models.

Apple joins the ranks of tech giants such as OpenAI, Meta and Anthropic, which are being sued in the United States for using protected literary works without authorisation in the development of its AI models known as "Apple Intelligence".

On 5 September 2025, two American authors filed a class action lawsuit in federal court in San Francisco, alleging a violation of the Copyright Act (17 U.S.C. § 501).

They are seeking damages, a permanent injunction, and are even demanding the destruction of the "Apple Intelligence" models, pursuant to section 503(b).

This case highlights fundamental issues surrounding the concept of "fair use" in American law, the use of "shadow libraries" to retrieve freely accessible digital media content that is normally subject to payment or controlled access without complying with these conditions, and, correlatively, the legal status of so-called "publicly accessible" data sets.



PERSONAL DATA NEWS

The General Court of the European Union has confirmed the validity of the Data Privacy Framework

General Court of the European Union, Philippe Latombe v European Commission, 23 September 2025, T-553/23

In a decision dated 23 September 2025, the General Court of the European Union confirmed the validity of the Data Privacy Framework (DPF), adopted by the European Commission on 10 July 2023, ruling that it ensures an adequate level of protection for personal data transferred to the United States. This decision provides a degree of legal certainty for European companies that use services involving transatlantic data transfers.

The DPF succeeds in the previous adequacy mechanisms, Safe Harbor and Privacy Shield, both of which were invalidated by the Court of Justice of the European Union due to guarantees deemed insufficient in light of the requirements of the GDPR and fundamental rights. In this case, MEP Philippe Latombe challenged the Commission's decision, arguing that the redress mechanisms provided for in the United States, in particular the Data Protection Review Court (DPRC), did not offer the necessary guarantees of independence and effectiveness.

The Court rejected these arguments, considering that the safeguards put in place by the US authorities were sufficient to ensure protection in line with European standards. It thus validated the Commission's approach, which had considered that developments in the US legal framework made it possible to restore an adequate level of protection.

However, this decision could be appealed before the Court of Justice of the European Union. It is part of a broader debate on the balance between national security and privacy protection in the context of international data flows.

CJEU clarifies the classification of pseudonymised data

CJEU, EDPS v SRB, 4 September 2025, C-413-23 P

On 4 September 2025, the Court of Justice of the European Union (CJEU) overturned the decision in the EDPS v SRB case, providing important clarifications on the classification of pseudonymised data under the GDPR and Regulation (EU) 2018/1725 on the processing of personal data by EU institutions and bodies. This decision is in line with case law that adopts a broad interpretation of the concept of personal data, as already affirmed in the Nowak, Breyer and IAB Europe judgments.

The CJEU points out that pseudonymised data can be considered personal data if there is a reasonable possibility of re-identification. However, it qualifies this approach by emphasising that the analysis must take into account the actual capabilities of the recipient and the practical obstacles to re-identification. This clarification marks an important development, as it introduces a pragmatic dimension to risk assessment, moving away from a purely theoretical approach. While this decision is seen as a positive sign for the protection of individuals, it also highlights the ongoing tensions between compliance requirements and the need for innovation.

PERSONAL DATA NEWS

Record fines for Google and Shein, sanctioned by the CNIL for their illegal practices in relation to cookies and advertising

CNIL, Deliberation concerning GOOGLE LLC and GOOGLE IRELAND LIMITED, 1 September 2025, SAN-2025-004

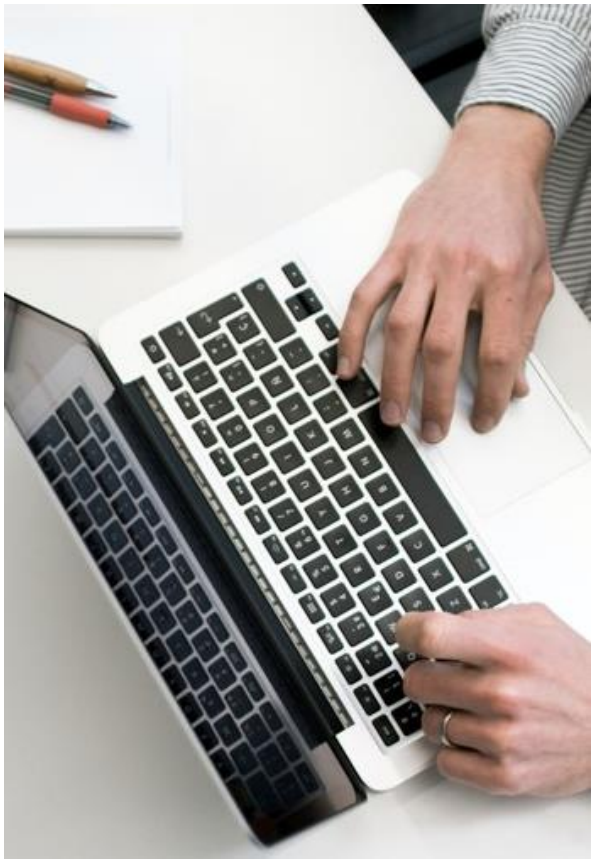
CNIL, Deliberation concerning INFINITE STYLES SERVICES CO. LIMITED, 1 September 2025, SAN-2025-005

The French Data Protection Authority (CNIL) has imposed two unprecedented penalties on Google and Shein for breaches relating to cookies and advertising. Google has been fined a record €325 million, while Shein will have to pay €150 million.

The CNIL punishes Google for two main practices. Firstly, displaying advertisements in Gmail without prior consent, inserted between emails sent to 53 million French users who had activated "smart features". These ads, visible in the 'Promotions' and 'Social Networks' tabs, are classified as direct marketing, requiring explicit consent. Secondly, a faulty "cookie wall": when creating a Google account, users were not clearly informed that access to services was conditional on the placement of advertising cookies, which contravenes Article 82 of the Data Protection Act.

Shein is being penalised for automatically placing advertising cookies as soon as users arrive on its website, without prior interaction, as well as for incomplete information banners and ineffective refusal mechanisms. Even after selecting "Refuse all", cookies continued to be placed, without any mention of the third parties involved.

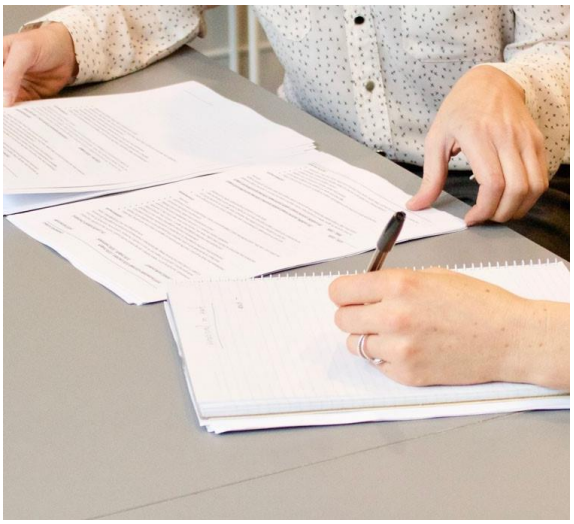
Google has six months to comply, or face a penalty of £100,000 per day. Shein has already corrected its practices. Both companies can appeal the decision within four months.



PERSONAL DATA NEWS

The EDPB adopts guidelines on the interaction between the DSA and the GDPR

EDPB, Guidelines on the interplay between the DSA and the GDPR, 11 September 2025, 3/2025

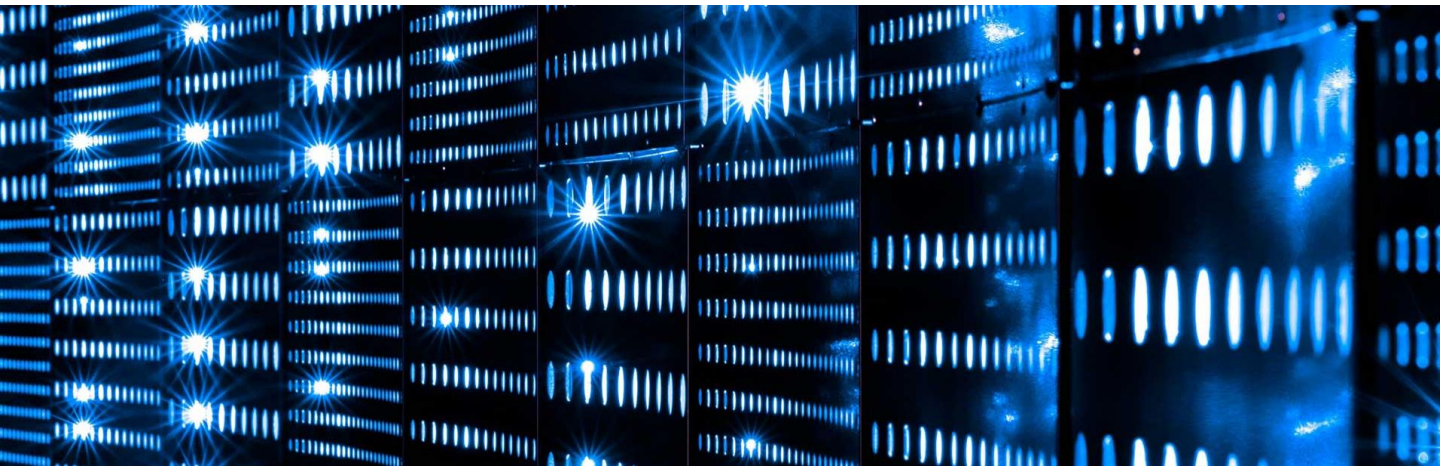


At its plenary meeting in September, the European Data Protection Board (EDPB) adopted guidelines aimed at clarifying the relationship between the DSA and the GDPR. This is the EDPB's first initiative dedicated to the interaction between these two texts, at a time when the European Union is strengthening its legal framework for the digital space.

The DSA aims to supplement the provisions of the GDPR in order to ensure a high level of protection of fundamental rights online, in particular freedom of expression and user safety. It applies mainly to intermediary services such as search engines and digital platforms. Several of its provisions concern the processing of personal data, which raises questions of interpretation and consistency with the GDPR.

The guidelines adopted by the EDPS aim to ensure harmonised application of the two regulations, particularly where the DSA refers to concepts and definitions from the GDPR. They reiterate that, although the interpretation of the DSA is a matter for the competent authorities and European courts, certain obligations imposed on intermediary service providers must be analysed in the light of data protection principles.

For example: *"The guidelines recognise that efforts to detect, identify and address (e.g. demonetise, remove or disable access to) illegal content under Article 7 of the DSA may involve the processing of personal data using various techniques. In addition to highlighting the specific risks to individuals that should be mitigated in the context of content moderation, the guidelines specify the conditions under which Article 6(1)(c) or (f) of the GDPR may serve as a legal basis for measures to detect, identify and disable illegal content."*



Entry into force of the Data Act on 12 September 2025

Regulation of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Regulation), 19 October 2022, 2022/2065

The Data Act came into force on 12 September 2025, marking a key milestone in the European data strategy. This regulation complements the Data Governance Act (DGA) in order to promote and regulate access to, sharing and reuse of data within the European Union. Together, these texts aim to create a harmonised framework that promotes innovation while ensuring the protection of users' rights.

Data is now the foundation of many digital products and services, particularly those resulting from the rise of the Internet of Things (IoT).

The Data Act aims to facilitate access to data generated by the use of connected products and services. It establishes rules enabling users – whether consumers or businesses – to retrieve, use and share the data they co-generate. Users must be able to view the data generated free of charge and reuse it for personal or professional purposes, including transferring it to other providers. Systems must ensure seamless data portability between services. Sharing agreements must comply with fair terms and conditions, without unduly restricting the use of data.

This applies to manufacturers of connected objects, associated service providers (cloud, SaaS), data holders, third-party recipients and end users (businesses or individuals).

In terms of penalties, each Member State must establish an appropriate enforcement framework by September 2025. In France, the SREN law already provides for fines of up to 3% of global turnover, or even 5% in the event of a repeat offence. GDPR or criminal penalties may also apply, depending on the case.

Companies must adapt their practices: mapping data flows, implementing access procedures, reviewing contracts, adjusting technical architectures, and strengthening confidentiality and trade secret protection policies.

PERSONAL DATA NEWS

The CJEU specifies the conditions under which a person may obtain compensation for non-material damage resulting from a breach of the GDPR

Court of Justice of the European Union, IP v Quirin Privatbank AG, 4 September 2025, C-655/23

The Court of Justice of the European Union (CJEU) recently clarified the conditions under which a person can obtain compensation for non-material damage resulting from a breach of the GDPR. This recognition is in line with case law which affirms that the loss of control over one's personal data can have psychological or emotional consequences that justify compensation.

In this case, a job applicant had his salary expectations mistakenly disclosed to a third party. The third party, who knew him, passed on the information to him, causing him to feel humiliated, fearful and unhappy. He considered that his reputation had been damaged and feared that his data would be misused. The CJEU ruled that if the person concerned can demonstrate that this disclosure constitutes a violation of the GDPR and that they have suffered moral damage as a result, compensation is due.

However, the Court specifies that this remedy must be complete and effective, without including punitive damages. In cases of minor harm, symbolic compensation or even an apology may suffice. In addition, the person concerned may also seek an injunction to prevent any future unlawful processing, if permitted by national law.

The Ministry of Economy and Finance has unveiled the list of competent authorities for artificial intelligence

Ministry of Economy, Finance, and Industrial, Energy and Digital Sovereignty, Competent authorities for the implementation of the European Regulation on Artificial Intelligence, 9 September 2025

On 9 September, in accordance with the Artificial Intelligence Regulation (RIA), the Ministry of Economy and Finance published the list of French national authorities competent in the field of AI and the distribution of their responsibilities, accompanied by the diagram below. The stated aim of this organisation is to ensure effective control of AI systems by administrations and sectoral agencies.

The CNIL will be responsible in particular for prohibited practices relating to real-time remote biometric identification for law enforcement purposes, as well as for high-risk systems used in workforce management. Systems deployed in critical infrastructure will fall under the remit of senior defence and security officials in the relevant ministries.

The DGCCRF is designated as the single point of contact for the operational coordination of market surveillance authorities, in accordance with Article 70(2) of the RIA. The Directorate-General for Enterprise (DGE) will be responsible for strategic coordination. In support of this, ANSSI and the Digital Regulation Expertise Centre (PEReN) will provide a pool of shared technical expertise for the compliance monitoring of AI systems.

This division of responsibilities still needs to be approved by Parliament as part of a draft law, marking an important step in the implementation of the European framework for artificial intelligence.

Stéphanie Berland

Avocate - Associée

T: +33 1 40 69 26 63

E: s.berland@dwf.law

Emmanuel Durand

Avocat - Associé

T: +33 1 40 69 26 83

E: e.durand@dwf.law

Florence Karila

Avocate - Associée

T: +33 1 40 69 26 57

E: f.karila@dwf.law

Anne-Sylvie Vassenaix-Paxton

Avocate - Associée

T: +33 1 40 69 26 51

E: as.vassenaix-paxton@dwf.law

DWF est l'un des principaux fournisseurs mondiaux de services juridiques et commerciaux intégrés.

Notre approche de Gestion Juridique Intégrée offre une plus grande efficacité, une maîtrise des prix et une transparence pour nos clients.

Nous fournissons des services juridiques et commerciaux intégrés à l'échelle mondiale grâce à nos 3 offres, Legal Advisory, Legal Operations et Business Services, dans nos huit secteurs clés. Nous combinons de manière transparente un certain nombre de nos services pour fournir des solutions sur mesure à nos différents clients.

dwfgroup.com