The Seqlense Regulatory Brief - Édition #8

Crypto &TradFi

Special Edition: AI Act × GDPR - Interplay, Case Law and Tensions

Decoding regulation for investors

From parallel tracks to integration

The previous edition of the Regulatory Brief ended on a key observation: the provisional political agreement of 7 May 2026 on the Digital Omnibus on AI postpones the application of several obligations relating to high-risk AI systems, subject to formal adoption of the text. However, this postponement does not suspend the application of the GDPR where personal data are processed. Several readers asked us to go further on a specific point: how does the AI Act articulate with the GDPR, and more broadly with European data protection law?

The question is denser than it appears. The AI Act and the GDPR overlap on three levels: a ratione materiae level, because many AI systems process personal data; a ratione personae level, because the AI Act's roles of provider and deployer only imperfectly map onto the GDPR's roles of controller and processor; and an institutional level, because the AI Office, national market surveillance authorities and data protection authorities (DPAs) must now cooperate within a landscape where competences are not always clearly delineated.

This special edition, in direct continuity with Brief 7, examines four structurally important angles of interplay: the formal position of European data protection authorities (EDPB/EDPS) on the Digital Omnibus on AI, the case law of the Court of Justice of the European Union on automated decisions (SCHUFA and Dun & Bradstreet), the practical interplay between the Fundamental Rights Impact Assessment (FRIA) provided for by the AI Act and the Data Protection Impact Assessment (DPIA) under the GDPR, and finally the CNIL's doctrine on the training of artificial intelligence models.

For financial actors, particularly those who develop or deploy AI systems for credit scoring, insurance pricing or customer due diligence, these four angles together form the most operational reading grid currently available.

The Weak Signal

The emergence of "joint guidelines" between the EDPB and the Commission is becoming the new operating model of European digital regulation

On 9 October 2025, the EDPB and the European Commission published, for public consultation, their first joint guidelines on the interplay between the Digital Markets Act (DMA) and the GDPR. This method of institutional coordination could become structuring for the future AI Act × GDPR joint guidelines expected in 2026. The EDPB has confirmed that it is working with the Commission, and more specifically with the AI Office, on these joint guidelines dedicated to the interplay between the AI Act and European data protection laws.

For regulated actors, this operating model is **more operational than it appears**. Individual opinions of the European Data Protection Board (EDPB) remain legally advisory, and the Commission's communications have their own scope. But when the two institutions **publish jointly**, they close off much of the space for divergent interpretation among national regulators. For legal and compliance departments, this is a signal to watch: the **AI Act × GDPR joint guidelines** expected in the coming months should, even more than the AI Omnibus itself, shape day-to-day practice.

This institutional movement is explicitly anchored in the EDPB's Helsinki Statement and its 2024-2027 strategy, one of the stated objectives of which is to facilitate GDPR compliance while strengthening cross-cutting coherence with other digital regulations.

Focus 1: The Joint EDPB-EDPS Opinion on the Digital Omnibus on AI

In January 2026, the EDPB and the European Data Protection Supervisor (EDPS) adopted their Joint Opinion 1/2026 on the proposal for a Digital Omnibus on AI. A second joint opinion (Joint Opinion 2/2026), covering the Digital Omnibus in its broader sense (amendments to the GDPR, the ePrivacy Directive, the Data Act, etc.), followed in February 2026.

A nuanced stance: support for the objectives, vigilance on fundamentals

Both institutions support the general objective of simplification pursued by the Commission's proposal and acknowledge the practical difficulties of applying the AI Act. However, they make substantial recommendations to ensure that simplification does not come at the expense of the level of protection of fundamental rights.

Four points of attention

📌 **1. Sensitive data used for bias detection**

The Omnibus provides for extending the legal basis for processing sensitive data for the purposes of detecting and correcting bias. The EDPB and the EDPS recommend that this use be strictly limited to situations where it is strictly necessary and where the risk of adverse effects linked to bias is sufficiently serious. They also recommend clarifications on the interplay between these provisions and the GDPR.

📌 **2. Postponement of high-risk obligations**

Both institutions express concerns about the postponement of high-risk obligations, insofar as this postponement concerns in particular the requirements regarding risk management, data governance and the quality of training datasets, all areas which directly affect the protection of personal data.

📌 **3. European regulatory sandboxes**

The proposal introduces, via the new Article 57(3a) of the AI Act, sandboxes operated by the AI Office for systems based on general-purpose AI models. The EDPB and the EDPS welcome this initiative but identify a gap: unlike the national sandboxes provided for in Article 57(10), no explicit provision organises the involvement of national data protection authorities in the European sandboxes. They recommend that the EDPB be granted (1) an advisory role in order to ensure coherence on data protection aspects and (2) observer status on the European Artificial Intelligence Board (AI Board).

📌 **4. AI literacy**

The EDPB and the EDPS underline that the "AI literacy" obligation within organisations, created by Article 4 of the AI Act, contributes to raising ethical and social awareness of the benefits and risks of AI. If the co-legislators decide to maintain a new obligation for the Commission and Member States to promote AI literacy, this should be added to the existing obligation of providers and deployers, not replace it.

Impact for regulated actors

- For legal and compliance departments, the joint opinion constitutes a **valuable doctrinal indicator**: it reveals the points on which European data protection authorities will maintain strong vigilance, regardless of how the Omnibus text ultimately evolves.
- For actors deploying AI systems that process personal data, the message is clear: **the postponement of high-risk obligations in no way reduces the application of the GDPR**. Processing of personal data in connection with the development or deployment of AI continues to fall fully and immediately within the scope of the GDPR.
- For actors wishing to use sensitive data for debiasing purposes, **the justification threshold remains high**: strict necessity, seriousness of the risk of discrimination, rigorous documentation. Mere "good intent" is not enough.

Focus 2: SCHUFA and Dun & Bradstreet - The Case Law

Two recent decisions of the Court of Justice of the European Union (CJEU) now form an interpretative bedrock for the regulation of automated decision-making systems, including those based on artificial intelligence. They primarily concern the financial sector, which relies heavily on automated scoring.

SCHUFA (C-634/21, 7 December 2023) - When a score may constitute an automated decision

The case opposed an individual to SCHUFA, the German credit assessment agency. The customer OQ had been refused a loan on the basis of a creditworthiness score generated by SCHUFA. She had

requested the erasure of, and access to, the data used; SCHUFA refused to disclose the mathematical formula and the exact logic of the calculation, invoking business secrecy.

In SCHUFA, the CJEU held that the automated generation of a creditworthiness score by a credit assessment agency may constitute an individual automated decision within the meaning of Article 22 of the GDPR, where that score plays a decisive role in the decision taken by a third party — in this instance, where the lending bank relies decisively on that value to establish, perform or terminate a contractual relationship. Classification therefore does not operate in abstracto but according to the actual role of the score in the third-party user's final decision.

The practical consequence remains significant: the obligation to comply with Article 22 of the GDPR is liable to weigh not only on the final lender, but also on the agency that produces the score where the conditions laid down by the Court are met. SCHUFA was not, however, compelled to disclose the exact mathematical weighting formula.

Dun & Bradstreet (C-203/22, 27 February 2025) - The content of "meaningful information"

On 27 February 2025, the CJEU clarified what "meaningful information about the underlying logic" within the meaning of Article 15(1)(h) of the GDPR must contain where the controller implements an automated decision.

The Court first confirmed the SCHUFA case law: the calculation of a credit score by an agency (in this case Dun & Bradstreet Austria, which had unfavourably assessed a person's capacity to enter into a telephony contract) constitutes an automated decision within the meaning of Article 22, even though the telephony operator formally remains the final decision-maker.

In Dun & Bradstreet, the CJEU clarified that the information provided to the data subject must enable them to understand the procedures and principles that led to the automated decision, without however requiring full disclosure of a mathematical formula or a protected algorithm. The controller must therefore provide concise, transparent, intelligible and easily accessible information on the "procedures and principles" applied, going beyond a mere general description, while being able to invoke the protection of trade secrets or copyright in the software so as not to disclose sensitive technical elements. These protections must be reconciled with the right of access, under the supervision of independent authorities or courts tasked with assessing the balance.

Why these two judgments structure AI compliance

- They **predate the AI Act in time** and provide the interpretative grid which the European legislator intends to adopt. Article 13 of the AI Act, which imposes technical documentation and explainability of high-risk systems, extends this logic of transparency.
- They establish that **the chain of responsibility extends from the provider of the model or score to the deployer**, which resonates strongly with the sharing of obligations between "provider" and "deployer" within the meaning of the AI Act.
- They establish a **minimum explainability standard** which does not permit complete opacity but does not, on the other hand, compel full disclosure of technical parameters. This zone of compromise is precisely the one that will be occupied by the future EDPB-Commission joint guidelines on AI Act × GDPR interplay.

Impact for professionals

- For **credit assessment agencies, scoring fintechs and AI model providers** used in credit-granting or insurance decisions, these two judgments confirm that they are fully bound by Article 22 of the GDPR, including where the final decision-maker is their client.
- For **banks and insurers** deploying third-party scoring systems, the Dun & Bradstreet case law implies providing the applicant, where access is requested, with a sufficiently substantive explanation of the decision's logic, going beyond a generic reference to the use of a score.
- The interplay with **Article 13 of the AI Act** on the transparency of high-risk systems becomes a point of attention: actors must build a coherent explanatory narrative, capable of being deployed both to respond to GDPR access requests and to AI Act requirements.

Focus 3: FRIA and DPIA - Practical Interplay of Impact Assessments

The AI Act creates, in its Article 27, a new obligation for certain deployers of high-risk AI systems: the Fundamental Rights Impact Assessment (FRIA). This obligation interplays closely with the Data Protection Impact Assessment (DPIA) provided for in Article 35 of the GDPR, and this interplay is one of the most operational topics for compliance departments.

Comparative scope of the two assessments

- The **DPIA** (Article 35 GDPR) is required where processing is likely to result in a high risk to the rights and freedoms of natural persons. It is centred on the protection of personal data (Articles 7 and 8 of the Charter of Fundamental Rights).
- The **FRIA** (Article 27 AI Act) is required for deployers of high-risk AI systems listed in Annex III, and more specifically, according to the most widely shared reading, for public bodies and private actors providing public services, as well as for deployers of certain systems listed in particular at points 5(b) and 5(c) (credit scoring, life/health insurance pricing). It covers **all fundamental rights under the Charter**: non-discrimination, human dignity, access to justice, freedom of expression — and may apply even in the absence of personal data processing.

The bridge of Article 27(4)

Article 27(4) of the AI Act explicitly provides that, where a deployer has already carried out a DPIA in connection with the AI system concerned, it may rely on it to satisfy the FRIA obligations, the FRIA then “complementing” the DPIA. Reciprocally, Article 26(9) requires deployers to use the instructions provided by the AI system's provider to carry out their own DPIA obligations under the GDPR.

This architecture invites, in practice, an integrated approach: conducting a single assessment, broad enough to cover both data protection risks and the full range of fundamental rights. The duplication of assessments is explicitly presented by the AI Act as avoidable, subject however to ensuring that all rights covered by the Charter are effectively examined, and not merely data protection.

Five questions that the FRIA adds compared with the DPIA

- **Which fundamental rights** are likely to be affected by the deployment of the AI system?
- **Which categories of persons** are concerned, including persons who do not directly interact with the system (spillover effects)?
- **What is the frequency and scope of use** of the system (volume, periodicity, context)?
- **What specific risks** of discrimination, infringement of dignity, restricted access to services or deprivation of effective remedies are identified?
- **What governance, human oversight and remedial measures** are put in place?

FRIA template: an awaited instrument

Article 27(5) of the AI Act provides that the AI Office will publish a template intended to facilitate the conduct of FRIAs. This template had not yet been published at the date of the regulation's initial adoption and constitutes, in the calendar reshaped by the Omnibus, one of the technical deliverables expected in view of the 2 December 2027 application of obligations applicable to Annex III systems.

Impact for compliance departments

- For **banks, insurers and asset managers** deploying high-risk AI systems (credit scoring, life/health insurance pricing), organisations should build an integrated FRIA + DPIA assessment where the AI system is both high-risk within the meaning of the AI Act and likely to entail a high risk to rights and freedoms within the meaning of Article 35 of the GDPR. This integration does not mean that the two exercises are perfectly superimposable: the FRIA covers all fundamental rights under the Charter, whereas the DPIA is centred on data protection.
- For **public and para-public actors** deploying high-risk systems (social services, border control, justice, law enforcement), the FRIA is **explicitly mandatory** and must be notified to the national market surveillance authority.
- For all organisations, the FRIA introduces a structurally new question: **the impact of a system on persons who do not interact with it** — for example, an automated triage system that modifies access conditions to a public service for a category of persons indirectly targeted.

Cross-Cutting Reading: Three Friction Zones, Three Complementarity Zones

Three friction zones to anticipate

- The **question of supervisory competences**. The AI Act centralises certain supervisions (AI Office for systems based on GPAI models developed by the same provider), whereas the GDPR relies on national authorities (DPAs). Cooperation between the AI Office, national market surveillance authorities and DPAs is not yet fully organised; the EDPB and the EDPS expressly underline this.
- The **articulation of legal bases**. Processing personal data to develop an AI model requires a GDPR legal basis (often legitimate interest, sometimes consent, more rarely legal obligation or

public interest mission). This choice must be **compatible** with AI Act obligations, but the AI Act does not itself create a legal basis.

- The **regime of sensitive data for bias detection**. The Omnibus provides for broadening this possibility, but the EDPB/EDPS insist on its strictly necessary character. This tension is one of the points that should be clarified in the forthcoming joint guidelines.

Three zones of operational complementarity

- The **sharing of roles provider / deployer (AI Act) and controller / processor (GDPR)**, although not identical, makes it possible to build a coherent responsibility matrix, provided the analysis is conducted system by system.
- The **FRIA + DPIA integration**, explicitly permitted by Article 27(4) of the AI Act, may ease the compliance burden, subject to all fundamental rights covered by the FRIA being effectively examined and not just data protection. The two exercises do not perfectly overlap: they remain legally distinct.
- The **articulation of transparency obligations**: Article 13 of the AI Act (technical documentation of high-risk systems), Article 50 of the AI Act (information about interaction and marking of generated content), and Articles 13, 14 and 15 of the GDPR (prior information and right of access). Building a unified reference framework will be a key compliance challenge.

Main sources

- EDPB-EDPS, *Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, January 2026, edpb.europa.eu.
- EDPB-EDPS, *Joint Opinion 2/2026 on the Digital Omnibus* (GDPR, ePrivacy, Data Act, NIS2), February 2026, edpb.europa.eu.
- EDPB & European Commission, *Joint Guidelines on the interplay between the Digital Markets Act and the GDPR*, draft published on 9 October 2025 for public consultation.
- CJEU, judgment of 7 December 2023, *SCHUFA Holding (Scoring)*, Case C-634/21.
- CJEU, judgment of 27 February 2025, *Dun & Bradstreet Austria*, Case C-203/22.
- CNIL, *Recommendations on the development of AI systems — thirteen practical sheets*, publications 2024-2025, cnil.fr (in particular the “legitimate interest” and “web scraping” sheets of 19 June 2025).
- EDPB, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, December 2024.
- Regulation (EU) 2024/1689 (AI Act), in particular Articles 4 (AI literacy), 10 (data governance), 13 (transparency), 26 (deployers' obligations), 27 (FRIA), 50 (transparency).

- Regulation (EU) 2016/679 (GDPR), in particular Articles 5 (principles), 6 (legal bases), 9 (special categories), 13-14 (information), 15(1)(h) (right of access, logic of automated decisions), 22 (automated decisions), 35 (DPIA).
- EDPB Helsinki Statement (2024) and EDPB Strategy 2024-2027