Crypto &TradFi

Spécial AI Act × RGPD : Articulation, jurisprudence et tensions

Décrypter la réglementation pour les investisseurs

Du parallèle à l'intégration

L'édition précédente du Regulatory Brief s'arrêtait sur un constat : l'accord politique provisoire du 7 mai 2026 sur le Digital Omnibus on AI reporte l'application de plusieurs obligations relatives aux systèmes d'IA à haut risque, sous réserve de l'adoption formelle du texte. Ce report ne suspend toutefois pas l'application du RGPD lorsque des données personnelles sont traitées. Plusieurs lecteurs nous ont demandé d'aller plus loin sur un point précis : comment l'AI Act s'articule-t-il avec le RGPD, et plus largement avec le droit européen de la protection des données ?

La question est plus dense qu'il n'y paraît. L'AI Act et le RGPD se chevauchent en effet sur trois plans : un plan ratione materiae, parce qu'un grand nombre de systèmes d'IA traitent des données personnelles ; un plan ratione personae, parce que les rôles de fournisseur et de déployeur de l'AI Act ne recoupent qu'imparfaitement ceux de responsable de traitement et sous-traitant du RGPD ; et un plan institutionnel, parce que l'AI Office, les autorités nationales de marché et les autorités de protection des données (DPA) doivent désormais coopérer dans un paysage où les compétences ne sont pas toujours clairement délimitées.

Cette édition spéciale, en continuité directe avec le Brief 7, examine quatre angles d'articulation aujourd'hui structurants : la position formelle des autorités de protection des données européennes (EDPB/EDPS) sur le Digital Omnibus IA, la jurisprudence de la Cour de justice de l'Union européenne en matière de décisions automatisées (SCHUFA et Dun & Bradstreet), l'articulation pratique entre la Fundamental Rights Impact Assessment (FRIA) prévue par l'AI Act et la Data Protection Impact Assessment (DPIA) du RGPD, et enfin la doctrine de la CNIL sur l'entraînement des modèles d'intelligence artificielle.

Pour les acteurs financiers, en particulier ceux qui développent ou déploient des systèmes d'IA pour le scoring de crédit, la tarification d'assurance ou la connaissance client, ces quatre angles forment ensemble la grille de lecture la plus opérationnelle aujourd'hui disponible.

Le signal faible

L'émergence des « joint guidelines » entre l'EDPB et la Commission est en train de devenir le nouveau mode opératoire de la régulation numérique européenne

Le 9 octobre 2025, l'EDPB et la Commission européenne ont publié, pour consultation publique, leurs premières lignes directrices conjointes sur l'articulation entre le Digital Markets Act (DMA) et le RGPD. Cette méthode de coordination institutionnelle pourrait devenir structurante pour les futures lignes directrices AI Act × RGPD attendues en 2026. L'EDPB a confirmé travailler avec la Commission, et plus précisément avec l'AI Office, sur ces lignes directrices conjointes consacrées à l'articulation entre l'AI Act et les lois européennes de protection des données.

Pour les acteurs régulés, ce mode opératoire est **plus opérationnel qu'il n'y paraît**. Les opinions individuelles du Comité européen de la protection des données (EDPB) restent juridiquement consultatives, et les communications de la Commission ont une portée propre. Mais lorsque les deux institutions **publient ensemble**, elles ferment une grande partie des espaces d'interprétation divergente entre régulateurs nationaux. Pour les directions juridiques et conformité, c'est un signal à suivre : les **joint guidelines AI Act × RGPD** attendues dans les prochains mois devraient, plus encore que l'Omnibus IA lui-même, structurer la pratique quotidienne.

Ce mouvement institutionnel est explicitement adossé au Helsinki Statement de l'EDPB et à sa stratégie 2024-2027, dont l'un des objectifs assumés est de faciliter la conformité au RGPD tout en renforçant la cohérence transverse avec les autres réglementations numériques.

Focus 1 : L'opinion conjointe EDPB-EDPS sur le Digital Omnibus IA

En janvier 2026, l'EDPB et le Contrôleur européen de la protection des données (EDPS) ont adopté leur Joint Opinion 1/2026 sur la proposition de Digital Omnibus on AI. Une seconde opinion conjointe (Joint Opinion 2/2026), portant sur le Digital Omnibus dans son sens large (modifications du RGPD, de la directive ePrivacy, du Data Act, etc.), a suivi en février 2026.

Une posture nuancée : soutien aux objectifs, vigilance sur les fondamentaux

Les deux institutions soutiennent l'objectif général de simplification poursuivi par la proposition de la Commission et reconnaissent les difficultés pratiques d'application de l'AI Act. Toutefois, elles formulent des recommandations substantielles afin que la simplification ne se fasse pas au détriment du niveau de protection des droits fondamentaux.

Quatre points d'attention

📌 1. Données sensibles utilisées pour la détection des biais

L'Omnibus prévoit d'étendre la base juridique du traitement de données sensibles aux fins de détection et de correction des biais. L'EDPB et l'EDPS recommandent que cette utilisation soit strictement circonscrite aux situations où elle est strictement nécessaire et où le risque d'effets

négatifs liés aux biais est suffisamment sérieux. Ils recommandent également des clarifications sur l'articulation entre ces dispositions et le RGPD.

📌 2. Postponement des obligations haut risque

Les deux institutions expriment des préoccupations sur le report des obligations haut risque, dans la mesure où ce report concerne notamment les exigences en matière de gestion des risques, de gouvernance des données et de qualité des jeux de données d'entraînement, autant de domaines qui touchent directement à la protection des données personnelles.

📌 3. Bacs à sable réglementaires européens

La proposition introduit, via le nouvel article 57(3a) de l'AI Act, des bacs à sable opérés par l'AI Office pour les systèmes basés sur des modèles d'IA à usage général. L'EDPB et l'EDPS saluent cette initiative, mais identifient un manque : contrairement aux bacs à sable nationaux prévus par l'article 57(10), aucune disposition explicite n'organise l'implication des autorités nationales de protection des données dans les bacs à sable européens. Ils recommandent que l'EDPB se voie reconnaître (1) un rôle consultatif afin d'assurer la cohérence sur les aspects de protection des données et (2) un statut d'observateur au Conseil européen de l'intelligence artificielle (AI Board).

📌 4. AI literacy

L'EDPB et l'EDPS soulignent que l'obligation d'« AI literacy » au sein des organisations, créée par l'article 4 de l'AI Act, contribue à accroître la conscience éthique et sociale des bénéfices et des risques de l'IA. Si les co-législateurs décident de maintenir une nouvelle obligation pour la Commission et les États membres de promouvoir la maîtrise de l'IA, celle-ci doit s'ajouter à l'obligation existante des fournisseurs et déployeurs, et non s'y substituer.

Impact pour les acteurs régulés

- Pour les directions juridiques et conformité, l'opinion conjointe constitue un **précieux indicateur de doctrine** : elle révèle les points sur lesquels les autorités de protection des données européennes maintiendront une vigilance forte, indépendamment de l'évolution finale du texte Omnibus.
- Pour les acteurs déployant des systèmes d'IA traitant des données personnelles, le message est clair : **le report des obligations à haut risque ne réduit en rien l'application du RGPD**. Les traitements de données personnelles dans le cadre du développement ou du déploiement d'IA continuent de relever pleinement et immédiatement du RGPD.
- Pour les acteurs souhaitant utiliser des données sensibles pour des objectifs de débiaisage, **le seuil de justification reste élevé** : nécessité stricte, gravité du risque de discrimination, documentation rigoureuse. La simple « bonne intention » ne suffit pas.

Focus 2 : SCHUFA et Dun & Bradstreet – La jurisprudence

Deux décisions récentes de la Cour de justice de l'Union européenne (CJUE) constituent désormais un socle interprétatif de la régulation des systèmes décisionnels automatisés, y compris ceux fondés sur l'intelligence artificielle. Elles concernent au premier chef le secteur financier, qui recourt massivement au scoring automatisé.

SCHUFA (C-634/21, 7 décembre 2023) - Quand le score peut constituer une décision automatisée

L'affaire opposait un particulier à SCHUFA, agence allemande d'évaluation du crédit. Le client OQ s'était vu refuser un prêt sur la base d'un score de solvabilité généré par SCHUFA. Elle avait demandé l'effacement et l'accès aux données utilisées ; SCHUFA refusait de communiquer la formule mathématique et la logique exacte du calcul, invoquant le secret des affaires.

Dans SCHUFA, la CJUE a jugé que la génération automatisée d'un score de solvabilité par une agence d'évaluation du crédit peut constituer une décision individuelle automatisée au sens de l'article 22 du RGPD, lorsque ce score joue un rôle déterminant dans la décision prise par un tiers, en l'espèce, lorsque la banque prêteuse s'appuie de manière déterminante sur cette valeur pour établir, exécuter ou mettre fin à une relation contractuelle. La qualification ne s'opère donc pas in abstracto mais en fonction du rôle effectif du score dans la décision finale du tiers utilisateur.

La conséquence pratique reste significative : l'obligation de respecter l'article 22 du RGPD est susceptible de peser non plus seulement sur le prêteur final, mais aussi sur l'agence qui produit le score lorsque les conditions posées par la Cour sont réunies. SCHUFA n'a toutefois pas été contrainte de divulguer la formule mathématique exacte de pondération.

Dun & Bradstreet (C-203/22, 27 février 2025) - Le contenu de l'« information utile »

Le 27 février 2025, la CJUE a précisé ce que doit contenir l'« information utile sur la logique sous-jacente » au sens de l'article 15(1)(h) du RGPD, lorsque le responsable du traitement met en œuvre une décision automatisée.

La Cour confirme d'abord la jurisprudence SCHUFA : le calcul d'un score de crédit par une agence (en l'espèce Dun & Bradstreet Austria, qui avait évalué défavorablement la capacité d'une personne à conclure un contrat de téléphonie) constitue une décision automatisée au sens de l'article 22, même si l'opérateur de téléphonie reste formellement le décideur final.

Dans Dun & Bradstreet, la CJUE précise que l'information fournie à la personne concernée doit permettre de comprendre les procédures et principes ayant conduit à la décision automatisée, sans pour autant imposer la divulgation intégrale d'une formule mathématique ou d'un algorithme protégé. Le responsable du traitement doit ainsi délivrer une information concise, transparente, intelligible et facilement accessible sur les « procédures et principes » appliqués, au-delà d'une simple description générale, tout en pouvant invoquer la protection du secret des affaires ou du droit d'auteur sur le logiciel pour ne pas divulguer les éléments techniques sensibles. Ces

protections doivent être conciliées avec le droit d'accès, sous le contrôle d'autorités indépendantes ou de juridictions chargées d'apprécier l'équilibre.

Pourquoi ces deux arrêts structurent la conformité IA

- Ils **précèdent l'AI Act dans le temps** et fournissent la grille d'interprétation que le législateur européen entend reprendre à son compte. L'article 13 de l'AI Act, qui impose une documentation technique et une explicabilité des systèmes à haut risque, prolonge cette logique de transparence.
- Ils établissent que **la chaîne de responsabilité s'étend du fournisseur du modèle ou du score au déployeur**, ce qui résonne fortement avec le partage des obligations entre « fournisseur » et « déployeur » au sens de l'AI Act.
- Ils établissent un **standard d'explicabilité minimal** qui n'autorise pas l'opacité totale, mais ne contraint pas davantage à la divulgation intégrale des paramètres techniques. Cette zone de compromis est précisément celle qu'occuperont les futures lignes directrices conjointes EDPB-Commission sur l'articulation AI Act × RGPD.

Impact pour les professionnels

- Pour les **agences d'évaluation du crédit, fintechs de scoring et fournisseurs de modèles d'IA** utilisés dans des décisions d'octroi de crédit ou d'assurance, ces deux arrêts confirment qu'ils sont pleinement tenus par l'article 22 du RGPD, y compris quand le décideur final est leur client.
- Pour les **banques et assureurs** déployant des systèmes de scoring tiers, la jurisprudence Dun & Bradstreet implique de fournir au demandeur, en cas de demande d'accès, une explication suffisamment substantielle de la logique de la décision, au-delà d'une mention générique du recours à un score.
- L'articulation avec **l'article 13 de l'AI Act** sur la transparence des systèmes à haut risque devient un point d'attention : les acteurs doivent construire un récit explicatif cohérent, mobilisable à la fois pour répondre aux demandes d'accès RGPD et aux exigences de l'AI Act.

Focus 3 : FRIA et DPIA - Articulation pratique des évaluations d'impact

L'AI Act crée, à son article 27, une nouvelle obligation pour certains déployeurs de systèmes d'IA à haut risque : le Fundamental Rights Impact Assessment (FRIA), ou évaluation d'impact sur les droits fondamentaux. Cette obligation s'articule étroitement avec la Data Protection Impact Assessment (DPIA) prévue à l'article 35 du RGPD, et cette articulation est l'un des sujets les plus opérationnels pour les directions conformité.

Périmètre comparé des deux évaluations

- Le **DPIA** (article 35 RGPD) est requis dès lors qu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Il est centré sur la protection des données personnelles (articles 7 et 8 de la Charte des droits fondamentaux).
- Le **FRIA** (article 27 AI Act) est requis pour les déployeurs de systèmes d'IA à haut risque listés à l'annexe III, et plus particulièrement, selon la lecture la plus partagée, pour les organismes publics et les acteurs privés fournissant des services publics, ainsi que pour les déployeurs de certains systèmes listés notamment aux points 5(b) et 5(c) (scoring de crédit, tarification d'assurance vie/santé). Il couvre **l'ensemble des droits fondamentaux de la Charte** : non-discrimination, dignité humaine, accès à la justice, liberté d'expression et peut s'appliquer même en l'absence de traitement de données personnelles.

La passerelle de l'article 27(4)

L'article 27(4) de l'AI Act prévoit explicitement que, lorsqu'un déployeur a déjà accompli un DPIA en lien avec le système d'IA concerné, il peut s'en prévaloir pour satisfaire aux obligations FRIA, celui-ci venant alors « compléter » le DPIA. Réciproquement, l'article 26(9) impose aux déployeurs d'utiliser les instructions fournies par le fournisseur du système d'IA pour exécuter leurs propres obligations DPIA au titre du RGPD.

Cette architecture invite, en pratique, à une approche intégrée : conduire une seule évaluation, suffisamment large pour couvrir à la fois les risques de protection des données et l'ensemble des droits fondamentaux. La duplication des assessments est explicitement présentée par l'AI Act comme évitable, sous réserve, néanmoins, que tous les droits couverts par la Charte soient effectivement examinés et non pas seulement la protection des données.

Cinq questions que la FRIA ajoute par rapport à la DPIA

- **Quels droits fondamentaux** sont susceptibles d'être affectés par le déploiement du système d'IA ?
- **Quelles catégories de personnes** sont concernées, y compris des personnes qui n'interagissent pas directement avec le système (effet de débordement) ?
- **Quelle est la fréquence et la portée de l'usage** du système (volume, périodicité, contexte)?
- **Quels risques spécifiques** de discrimination, d'atteinte à la dignité, d'accès limité aux services ou de privation d'un recours effectif sont identifiés ?
- **Quelles mesures de gouvernance, de supervision humaine et de redressement** sont mises en place ?

Modèle de FRIA : un instrument attendu

L'article 27(5) de l'AI Act prévoit que l'AI Office publiera un modèle (template) destiné à faciliter la conduite des FRIA. Ce modèle n'avait pas encore été publié à la date d'adoption initiale du règlement et constitue, dans le calendrier remodelé par l'Omnibus, l'un des livrables techniques

attendus dans la perspective de l'application au 2 décembre 2027 des obligations applicables aux systèmes d'annexe III.

Impact pour les directions conformité

- Pour les **banques, assureurs et gestionnaires d'actifs** déployant des systèmes d'IA à haut risque (scoring de crédit, tarification d'assurance-vie/santé), les organisations devraient construire une évaluation intégrée FRIA + DPIA lorsque le système d'IA est à la fois à haut risque au sens de l'AI Act et susceptible d'entraîner un risque élevé pour les droits et libertés au sens de l'article 35 du RGPD. Cette intégration ne signifie pas que les deux exercices sont parfaitement superposables : le FRIA couvre l'ensemble des droits fondamentaux de la Charte, là où le DPIA est centrée sur la protection des données.
- Pour les **acteurs publics et parapublics** déployant des systèmes à haut risque (services sociaux, contrôle frontalier, justice, application de la loi), le FRIA est **explicitement obligatoire** et doit être notifié à l'autorité nationale de surveillance du marché.
- Pour l'ensemble des organisations, le FRIA introduit une question structurellement nouvelle : **l'impact d'un système sur des personnes qui n'interagissent pas avec lui**, par exemple, un système de tri automatisé qui modifie les conditions d'accès à un service public pour une catégorie de personnes ciblée indirectement.

Lecture transversale : trois zones de friction, trois zones de complémentarité

Trois zones de friction à anticiper

- La **question des compétences supervisorielles**. L'AI Act centralise certaines supervisions (AI Office pour les systèmes basés sur des modèles GPAI développés par le même fournisseur), tandis que le RGPD repose sur les autorités nationales (DPA). La coopération entre AI Office, autorités nationales de surveillance du marché et DPA n'est pas encore pleinement organisée ; l'EDPB et l'EDPS le soulignent expressément.
- L'**articulation des bases juridiques**. Conduire un traitement de données personnelles pour développer un modèle d'IA requiert une base juridique RGPD (souvent l'intérêt légitime, parfois le consentement, plus rarement l'obligation légale ou la mission d'intérêt public). Ce choix doit être **compatible** avec les obligations de l'AI Act, mais celui-ci ne crée pas en lui-même de base juridique.
- Le **régime des données sensibles pour la détection des biais**. L'Omnibus prévoit d'élargir cette possibilité, mais l'EDPB/EDPS insistent sur le caractère strictement nécessaire. Cette tension est l'un des points qui devraient être clarifiés dans les joint guidelines à venir.

Trois zones de complémentarité opérationnelle

- Le **partage des rôles fournisseur / déployeur (AI Act) et responsable / sous-traitant (RGPD)**, bien que non identique, permet de construire une matrice de responsabilités cohérente, à condition d'analyser système par système.
- L'**intégration FRIA + DPIA**, explicitement permise par l'article 27(4) de l'AI Act, peut alléger la charge de conformité sous réserve que tous les droits fondamentaux couverts par la FRIA soient effectivement examinés et non pas seulement la protection des données. Les deux exercices ne se superposent pas parfaitement : ils restent juridiquement distincts.

L'**articulation des obligations de transparence** : article 13 de l'AI Act (documentation technique du système haut risque), article 50 de l'AI Act (information de l'interaction et marquage des contenus générés), et articles 13, 14 et 15 du RGPD (information préalable et droit d'accès). Construire un référentiel

Sources principales

- 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)*, janvier 2026, edpb.europa.eu.
- EDPB-EDPS, *Joint Opinion 2/2026 on the Digital Omnibus* (RGPD, ePrivacy, Data Act, NIS2), février 2026, edpb.europa.eu.
- EDPB & Commission européenne, *Joint Guidelines on the interplay between the Digital Markets Act and the GDPR*, projet publié le 9 octobre 2025 pour consultation publique).
- CJUE, arrêt du 7 décembre 2023, *SCHUFA Holding (Scoring)*, affaire C-634/21.
- CJUE, arrêt du 27 février 2025, *Dun & Bradstreet Austria*, affaire C-203/22.
- CNIL, *Recommandations sur le développement des systèmes d'IA — treize fiches pratiques*, publications 2024-2025, cnil.fr (notamment fiches « intérêt légitime » et « web scraping » du 19 juin 2025.
- EDPB, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, décembre 2024.
- Règlement (UE) 2024/1689 (AI Act), notamment les articles 4 (AI literacy), 10 (gouvernance des données), 13 (transparence), 26 (obligations des déployeurs), 27 (FRIA), 50 (transparence).
- Règlement (UE) 2016/679 (RGPD), notamment les articles 5 (principes), 6 (bases juridiques), 9 (catégories particulières), 13-14 (information), 15(1)(h) (droit d'accès, logique des décisions automatisées), 22 (décisions automatisées), 35 (DPIA).
- Helsinki Statement de l'EDPB (2024) et Stratégie EDPB 2024-2027

Cette publication est fournie à titre strictement informatif et ne constitue ni un conseil en investissement, ni une recommandation personnalisée, ni une incitation à acheter ou vendre des instruments financiers ou des crypto-actifs.

Les informations présentées reflètent une analyse générale des dynamiques de marché et des évolutions réglementaires à la date de publication. Elles ne tiennent pas compte de la situation personnelle, des objectifs d'investissement ni du profil de risque de chaque lecteur.

Malgré les soins apportés à la sélection et à la vérification des sources, aucune garantie n'est donnée quant à l'exactitude, l'exhaustivité ou l'actualité des informations. Les marchés financiers et les crypto-actifs présentent des risques élevés, notamment de volatilité et de perte en capital.

En conséquence, toute décision d'investissement relève de la seule responsabilité du lecteur et doit, le cas échéant, être prise avec l'appui de conseillers professionnels qualifiés.