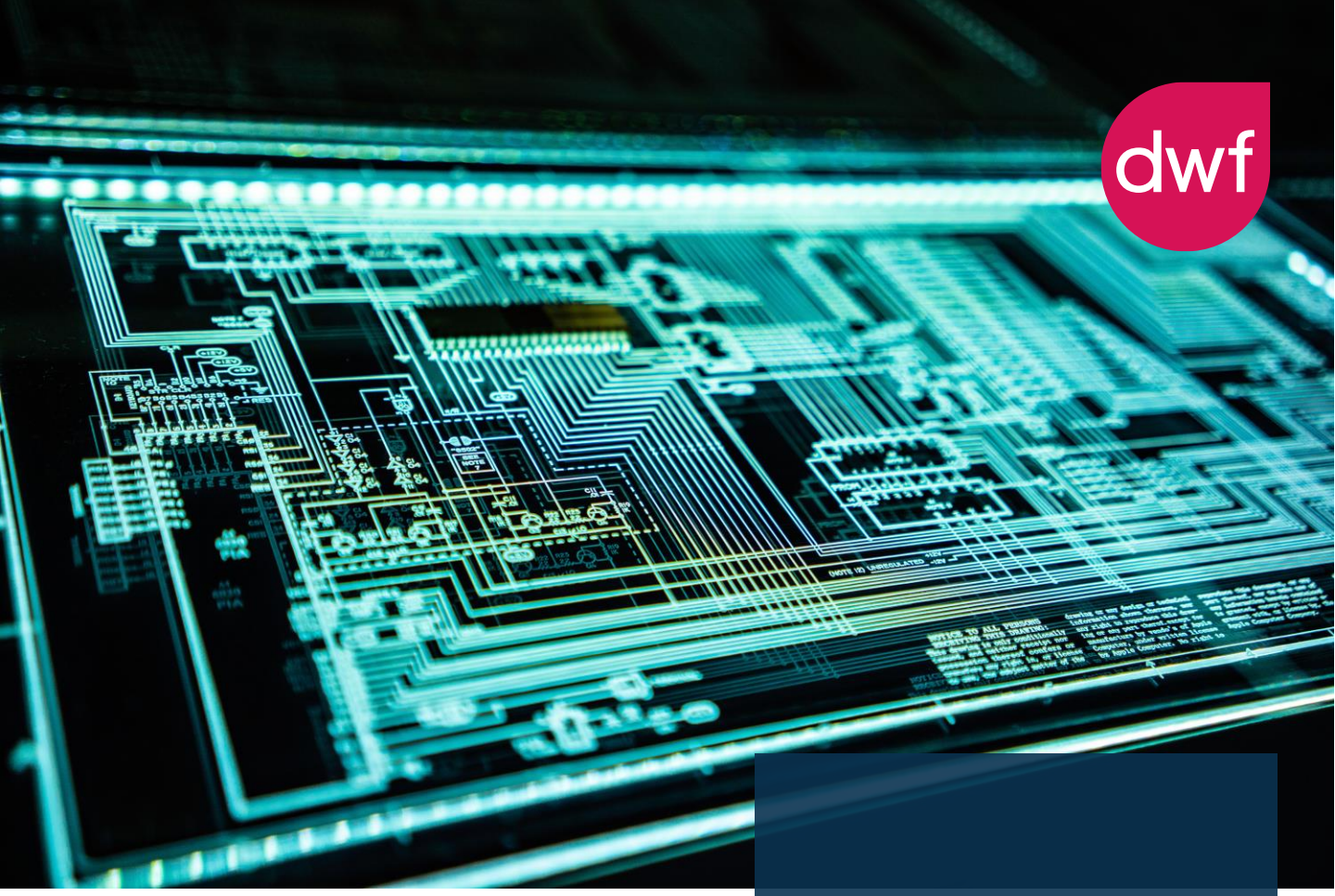


Newsletter

Tech / Data

Septembre - Octobre 2025

dwfgroup.com

Le Data Privacy Framework validé par l'UE

L'Union européenne confirme la validité du Data Privacy Framework, assurant la sécurité juridique des transferts de données vers les États-Unis (pour le moment)

Dans ce numéro

Dans ce numéro

ACTUALITES NOUVELLES TECHNOLOGIES

Etude sur l'interaction entre l'IA Act et le cadre législatif numérique de l'Union Européenne par le Parlement européen

Parlement Européen, Interaction entre la loi sur l'IA et le cadre législatif numérique de l'UE, 30 octobre 2025

Parlement Européen, Interaction entre la loi sur l'IA et le cadre législatif numérique de l'UE, 30 octobre 2025, En bref

Une étude du Parlement européen analyse les interactions entre l'IA Act et les principaux textes du cadre législatif numérique de l'Union européenne, notamment le RGPD, le DSA, le DMA, la CRA et la directive NIS2. Bien que chaque règlement poursuive un objectif légitime, leur combinaison soulève des préoccupations concernant la cohérence, la compétitivité et la capacité d'innovation du secteur européen de l'IA. Le cadre réglementaire, dense et stratifié, engendre des chevauchements, des lacunes et des incertitudes juridiques.

Parmi les tensions identifiées, la loi sur l'IA élargit la logique de sécurité des produits à des domaines complexes comme les droits fondamentaux, difficiles à évaluer avec les outils classiques de conformité. Elle s'applique à la fois aux fournisseurs et aux utilisateurs de systèmes d'IA, ce qui crée des chaînes de responsabilité complexes, particulièrement contraignantes pour les PME. Les systèmes à haut risque sont définis par des listes annexées et des critères subjectifs, ce qui introduit une ambiguïté juridique. Malgré l'existence de bacs à sable réglementaires et d'exemptions pour les logiciels open source, le cadre reste centré sur la gestion des risques, au détriment de l'innovation. De plus, le nouveau bureau de l'IA, chargé de superviser les GPAI et de coordonner l'application de la loi, empiète sur les compétences d'autorités déjà établies.

Les points de friction avec les autres textes sont nombreux : le RGPD impose des évaluations d'impact redondantes et des obligations de transparence qui se chevauchent ; le CRA et NIS2 introduisent des obligations similaires en cybersécurité ; le DSA et le DMA imposent des règles de transparence et de responsabilité parfois contradictoires pour les contenus générés par l'IA.

L'étude recommande, à court terme, de favoriser des orientations communes et la reconnaissance mutuelle des évaluations ; à moyen terme, de clarifier les rôles et simplifier les obligations ; à long terme, de construire un cadre numérique européen cohérent, propice à l'innovation tout en garantissant la protection des droits fondamentaux

ACTUALITES NOUVELLES TECHNOLOGIES

Charte du Tribunal des activités économiques de Paris afin d'encadrer l'utilisation des systèmes d'intelligence artificielle

Tribunal des Activités Economiques de Paris, Charte d'utilisation des systèmes d'intelligence artificielle et des données personnelles et sensibles au sein du tribunal des activités économiques de Paris, 9 septembre 2025

Le Tribunal des activités économiques de Paris a adopté une charte le 9 septembre 2025 pour encadrer l'usage de l'intelligence artificielle (IA) dans ses fonctions juridictionnelles et administratives. Ce texte vise à garantir une utilisation responsable, éthique et transparente de l'IA dans le cadre judiciaire.

La charte affirme que l'IA doit rester un outil d'assistance à la décision, et non un substitut à la réflexion humaine. Elle encourage une approche fondée sur la prudence, la mesure et la responsabilité. Les juges sont invités à utiliser ces technologies avec sobriété, uniquement dans le cadre de leurs missions, et en tenant compte de leur impact environnemental.

Les outils d'IA doivent être validés par le tribunal, et les magistrats sont tenus de vérifier l'exactitude des réponses générées. La protection des données personnelles et sensibles est centrale : les juges doivent respecter la politique de confidentialité, sécuriser les informations des justiciables et garantir la transparence de l'usage de l'IA. Les justiciables doivent être informés lorsque cela concerne leurs droits.

Un mécanisme de contrôle est prévu : toute anomalie doit être signalée au comité numérique, et les juges doivent suivre une formation dédiée à l'IA et à la protection des données. Cette charte incarne une volonté de concilier tradition juridique et innovation technologique, en promouvant une justice moderne, rigoureuse et respectueuse des droits fondamentaux dans un contexte numérique en constante évolution.

Sanction de la CNIL contre La Samaritaine des caméras dissimulées dans les réserves du magasin

CNIL, Délibération de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société SAMARITAINE SAS, 18 septembre 2025, n°SAN-2025-008

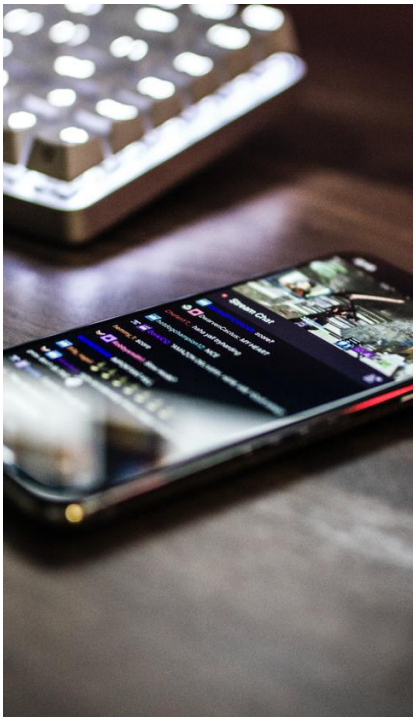
Le 18 septembre 2025, la CNIL a infligé une amende de 100 000 euros à la société SAMARITAINE SAS, exploitant le magasin du même nom, pour avoir installé des caméras dissimulées dans les réserves du magasin. Ces dispositifs, camouflés en détecteurs de fumée et équipés de micros, ont été mis en place en août 2023 pour lutter contre une recrudescence de vols. Découverts par les salariés, ils ont été retirés en septembre 2023.

Alertée par un article de presse et une plainte, la CNIL a mené un contrôle et relevé plusieurs manquements au RGPD :

1. Manquement à la loyauté et à la responsabilité : les caméras étaient dissimulées sans analyse préalable de conformité ni documentation sur leur caractère temporaire. Elles n'étaient pas mentionnées dans le registre des traitements ni dans une analyse d'impact, et la déléguée à la protection des données n'avait pas été informée.
2. Collecte excessive de données : les micros ont enregistré des conversations personnelles entre salariés, ce qui constitue une violation du principe de minimisation des données.
3. Non-association du DPO : la déléguée à la protection des données n'a été informée qu'après l'installation, alors qu'elle aurait pu conseiller sur les risques et les mesures à prendre.

La CNIL rappelle que l'usage de caméras dissimulées peut être admis dans des circonstances exceptionnelles, à condition de respecter un juste équilibre entre sécurité et vie privée, ce qui n'a pas été le cas ici.

ACTUALITES NOUVELLES TECHNOLOGIES



Transparence des contenus générés par IA : entrée en vigueur de l'étiquetage en Chine

Réglementation relative à la gestion de la synthèse profonde des services d'information sur Internet, 11 décembre 2022

En application de la règlementation en matière d'IA adoptée en 2022, la Chine impose depuis le 1er septembre 2025 un étiquetage obligatoire pour tout contenu généré ou modifié par intelligence artificielle, qu'il s'agisse de texte, d'image, de son, de vidéo ou de musique. Cette obligation découle des Measures for the Administration of Deep Synthesis Internet Information Services.

Le dispositif repose sur un double marquage :

- une indication visible pour l'utilisateur,
- un filigrane numérique ou des métadonnées garantissant la traçabilité.

Aucune exception n'est prévue, ni pour l'art, ni pour la satire : la transparence est érigée en principe absolu de loyauté numérique.

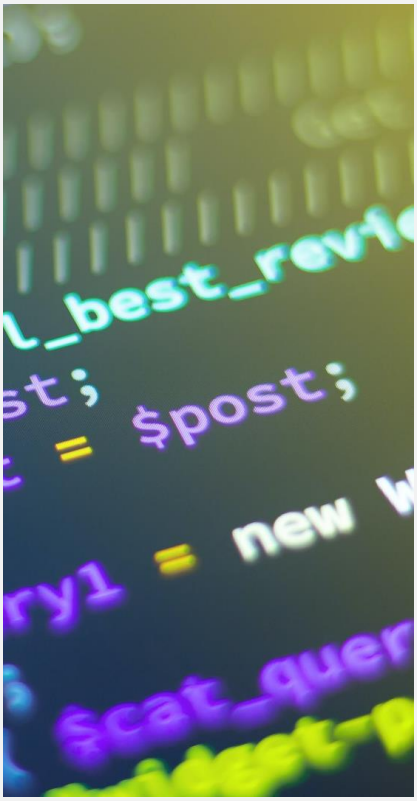
Action collective aux US contre Apple visant l'entraînement de ses modèles d'intelligence artificielle.

Apple rejoint le rang des géants technologiques tels que OpenAI, Meta ou encore Anthropic, poursuivis aux États-Unis pour avoir utilisé, sans autorisation, des œuvres littéraires protégées dans le cadre du développement de ses modèles d'IA dénommés « Apple Intelligence ».

Le 5 septembre 2025, deux auteurs américains ont déposé une plainte collective devant le tribunal fédéral de San Francisco, invoquant une violation du Copyright Act (17 U.S.C. § 501).

Ils demandent des dommages-intérêts, une injonction permanente, et vont jusqu'à réclamer la destruction des modèles « Apple Intelligence », en vertu de l'article 503(b).

Cette affaire met en lumière des questions fondamentales autour de la notion en droit américain du « fair use », de l'usage des « shadow libraries » consistant à récupérer les contenus de médias numériques librement accessibles mais normalement soumis à rémunération ou dont l'accès est contrôlé sans respecter ces conditions d'accès, et corrélativement du statut juridique des jeux de données dits « publiquement accessibles ».



ACTUALITES DONNEES PERSONNELLES

Le Tribunal de l'Union européenne a confirmé la validité du Data Privacy Framework

Tribunal de l'Union européenne, Philippe Latombe c/ Commission européenne, 23 septembre 2025, T-553/23

Dans une décision du 23 septembre 2025, le Tribunal de l'Union européenne a confirmé la validité du Data Privacy Framework (DPF), adopté par la Commission européenne le 10 juillet 2023, en jugeant qu'il garantit un niveau adéquat de protection des données personnelles transférées vers les États-Unis. Cette décision apporte une forme de stabilité juridique pour les entreprises européennes qui recourent à des services impliquant des transferts transatlantiques de données.

Le DPF succède aux précédents mécanismes d'adéquation, Safe Harbor et Privacy Shield, tous deux invalidés par la Cour de justice de l'Union européenne en raison de garanties jugées insuffisantes au regard des exigences du RGPD et des droits fondamentaux. Dans cette affaire, le député Philippe Latombe contestait la décision de la Commission, estimant que les mécanismes de recours prévus aux États-Unis, en particulier la Data Protection Review Court (DPRC), ne présentaient pas les garanties d'indépendance et d'efficacité requises.

Le Tribunal rejette ces arguments, considérant que les garanties mises en place par les autorités américaines sont suffisantes pour assurer une protection conforme aux standards européens. Il valide ainsi l'approche de la Commission, qui avait estimé que les évolutions du cadre juridique américain permettaient de rétablir un niveau de protection adéquat.

Cette décision pourrait toutefois faire l'objet d'un recours devant la Cour de justice de l'Union européenne. Elle s'inscrit dans un débat plus large sur l'équilibre entre sécurité nationale et protection de la vie privée dans le contexte des flux de données internationaux.

Précisions de la CJUE sur la qualification des données pseudonymisées

CJUE, EDPS c/ SRB, 4 septembre 2025, C-413-23 P

Le 4 septembre 2025, la Cour de justice de l'Union européenne (CJUE) a annulé la décision rendue dans l'affaire EDPS contre SRB, apportant des précisions majeures sur la qualification des données pseudonymisées au regard du RGPD et du Règlement (UE) 2018/1725 sur les traitements de données personnelles par les institutions et organismes de l'UE. Cette décision s'inscrit dans la continuité d'une jurisprudence qui adopte une interprétation large de la notion de données personnelles, déjà affirmée dans les arrêts Nowak, Breyer et IAB Europe.

La CJUE rappelle que les données pseudonymisées peuvent être considérées comme des données personnelles dès lors qu'il existe une possibilité raisonnable de réidentification. Toutefois, elle nuance cette approche en soulignant que l'analyse doit tenir compte des capacités concrètes du destinataire et des obstacles pratiques à la réidentification. Cette précision marque une évolution importante, car elle introduit une dimension pragmatique dans l'évaluation du risque, en s'éloignant d'une conception purement théorique. Si cette décision est perçue comme un signal positif pour la protection des personnes, elle met également en lumière les tensions persistantes entre exigences de conformité et besoins d'innovation.

ACTUALITES DONNEES PERSONNELLES

Amendes records pour Google et Shein, sanctionnés par la CNIL pour leurs pratiques illicites en matière de cookies et de publicités

CNIL, Délibération concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED, 1er septembre 2025, SAN-2025-004

CNIL, Délibération concernant la société INFINITE STYLES SERVICES CO. LIMITED, 1er septembre 2025, SAN-2025-005

La Commission nationale de l'informatique et des libertés (CNIL) a prononcé deux sanctions d'une ampleur inédite à l'encontre de Google et Shein pour des manquements liés aux cookies et à la prospection publicitaire. Google se voit infliger une amende record de 325 millions d'euros, tandis que Shein devra s'acquitter de 150 millions d'euros.

Concernant Google, la CNIL reproche deux pratiques principales. D'une part, l'affichage de publicités dans Gmail sans consentement préalable, insérées entre les courriels de 53 millions d'utilisateurs français ayant activé les « fonctionnalités intelligentes ». Ces annonces, visibles dans les onglets « Promotions » et « Réseaux sociaux », sont qualifiées de prospection directe, nécessitant un accord explicite. D'autre part, un « cookie wall » défaillant : lors de la création d'un compte Google, les utilisateurs n'étaient pas clairement informés que l'accès aux services était conditionné au dépôt de cookies publicitaires, ce qui contrevient à l'article 82 de la loi Informatique et Libertés.

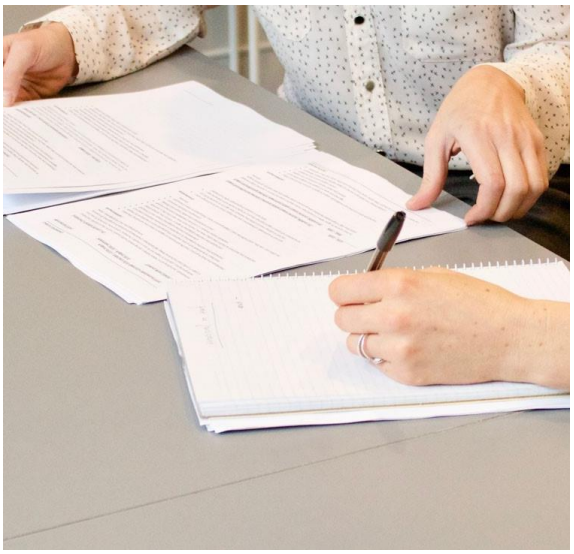
Shein est sanctionné pour le dépôt automatique de cookies publicitaires dès l'arrivée sur son site, sans interaction préalable, ainsi que pour des bandeaux d'information incomplets et des mécanismes de refus inefficaces. Même après avoir sélectionné « Tout refuser », des cookies continuaient d'être déposés, sans mention des tiers impliqués.

Google dispose de six mois pour se mettre en conformité, sous peine d'une astreinte de 100 000 euros par jour. Shein a déjà corrigé ses pratiques. Les deux entreprises peuvent contester la décision dans un délai de quatre mois.

ACTUALITES DONNEES PERSONNELLES

Le CEDP adopte des lignes directrices concernant l'interaction entre le DSA et le RGPD

CEDP, Guidelines on the interplay between the DSA and the GDPR, 11 septembre 2025, 3/2025



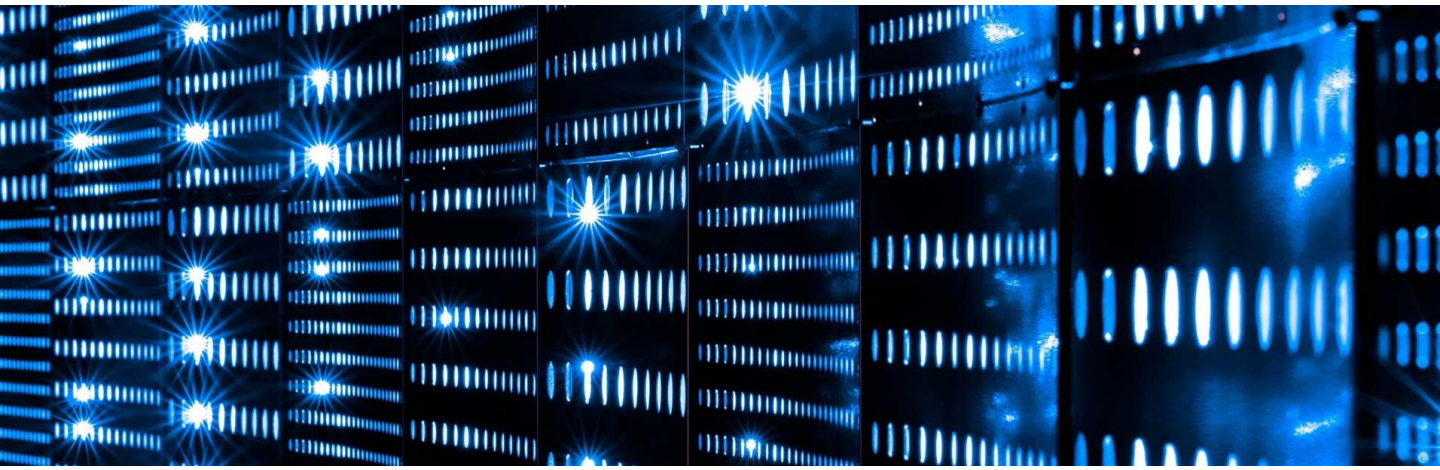
Lors de sa réunion plénière de septembre, le Comité européen de la protection des données (CEPD) a adopté des lignes directrices visant à clarifier l'articulation entre le DSA et le RGPD. Il s'agit de la première initiative du CEPD consacrée à l'interaction entre ces deux textes, dans un contexte où l'Union européenne renforce son cadre juridique pour l'espace numérique.

Le DSA a pour objectif de compléter les dispositions du RGPD afin de garantir un niveau élevé de protection des droits fondamentaux en ligne, notamment la liberté d'expression et la sécurité des utilisateurs. Il s'applique principalement aux services intermédiaires tels que les moteurs de recherche et les plateformes numériques. Plusieurs de ses dispositions concernent le traitement de données à caractère personnel, ce qui soulève des questions d'interprétation et de cohérence avec le RGPD.

Les lignes directrices adoptées par le CEPD visent à assurer une application harmonisée des deux réglementations, en particulier lorsque le DSA renvoie à des concepts et définitions issus du RGPD. Elles rappellent que, bien que l'interprétation du DSA relève des autorités compétentes et des juridictions européennes, certaines obligations imposées aux prestataires de services intermédiaires doivent être analysées à la lumière des principes de protection des données.

A titre d'exemple :" *Les lignes directrices reconnaissent que les efforts visant à détecter, identifier et traiter (par exemple, démonétiser, supprimer ou désactiver l'accès à) des contenus illégaux en vertu de l'article 7 du DSA peuvent impliquer le traitement de données à caractère personnel à l'aide de différentes techniques. Outre le fait de mettre en évidence les risques spécifiques pour les personnes qui devraient être atténués dans le contexte de la modération des contenus, les lignes directrices précisent dans quelles conditions l'article 6, paragraphe 1, point c) ou (f) du RGPD peut servir de base légale pour les mesures visant à détecter, identifier et désactiver les contenus illicites".*

ACTUALITES DONNEES PERSONNELLES



Entrée en application du Data Act le 12 septembre 2025

Règlement du parlement européen et du conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), 19 octobre 2022, 2022/2065

Le Data Act est entré en application le 12 septembre 2025, marquant une étape clé dans la stratégie européenne en matière de données. Ce règlement complète le Data Governance Act (DGA) afin de promouvoir et encadrer l'accès, le partage et la réutilisation des données au sein de l'Union européenne. Ensemble, ces textes visent à créer un cadre harmonisé favorisant l'innovation tout en garantissant la protection des droits des utilisateurs.

Les données constituent aujourd'hui le socle de nombreux produits et services numériques, en particulier ceux issus de l'essor des objets connectés (IoT).

Le Data Act vise à faciliter l'accès aux données générées par l'utilisation de produits et services connectés. Il instaure des règles permettant aux utilisateurs – qu'il s'agisse de consommateurs ou d'entreprises – de récupérer, utiliser et partager les données qu'ils co-génèrent. Les utilisateurs doivent pouvoir consulter gratuitement les données générées et les réutiliser à des fins personnelles ou professionnelles, y compris les transmettre à d'autres prestataires. Les systèmes doivent garantir une portabilité fluide des données entre services. Les contrats de partage doivent respecter des conditions équitables, sans restreindre abusivement l'usage des données.

Sont concernés : les fabricants d'objets connectés, les fournisseurs de services associés (cloud, SaaS), les détenteurs de données, les tiers destinataires, ainsi que les utilisateurs finaux (entreprises ou particuliers).

En matière de sanctions, chaque État membre doit prévoir un cadre répressif adapté d'ici septembre 2025. En France, la loi SREN prévoit déjà des amendes pouvant atteindre 3% du chiffre d'affaires mondial, voire 5% en cas de récidive. Des sanctions RGPD ou pénales peuvent aussi s'appliquer selon les cas.

Les entreprises doivent adapter leurs pratiques : cartographie des flux de données, mise en place de procédures d'accès, révision des contrats, ajustement des architectures techniques, et renforcement des politiques de confidentialité et de protection des secrets d'affaires.

ACTUALITES DONNEES PERSONNELLES

La CJUE précise les conditions dans lesquelles une personne peut obtenir réparation pour un dommage moral résultant d'une violation du RGPD

Cour de justice de l'Union européenne, IP c/ Quirin Privatbank AG, 4 septembre 2025, C-655/23

La Cour de justice de l'Union européenne (CJUE) a récemment précisé les conditions dans lesquelles une personne peut obtenir réparation pour un dommage moral résultant d'une violation du RGPD. Cette reconnaissance s'inscrit dans une jurisprudence qui affirme que la perte de contrôle sur ses données personnelles peut engendrer des conséquences psychologiques ou émotionnelles justifiant une indemnisation.
En l'espèce, un candidat à un emploi a vu ses prétentions salariales divulguées par erreur à une tierce personne. Cette dernière, le connaissant, lui retransmet l'information, suscitant chez lui un sentiment d'humiliation, de crainte et de mécontentement. Il estime avoir subi une atteinte à sa réputation et craindre une utilisation abusive de ses données. La CJUE estime que si la personne concernée démontre que cette divulgation constitue une violation du RGPD et qu'elle a subi un préjudice moral en conséquence, une réparation est due.
Toutefois, la Cour précise que cette réparation doit être complète et effective, sans pour autant inclure de dommages-intérêts punitifs. En cas de préjudice mineur, une indemnité symbolique ou même des excuses peuvent suffire. Par ailleurs, la personne concernée peut également demander une injonction pour empêcher tout traitement illicite futur, si le droit national le permet.

Le ministère de l'Économie et des finances a dévoilé la liste des autorités compétentes en matière d'intelligence artificielle

Ministère de l'économie, des finances, et de la souveraineté industrielle, énergétique et numérique, Les autorités compétentes pour la mise en œuvre du règlement européen sur l'intelligence artificielle, 9 septembre 2025

Le 9 septembre, conformément au Règlement sur l'intelligence artificielle (RIA), le ministère de l'Économie et des Finances a publié la liste des autorités nationales françaises compétentes en matière d'IA ainsi que la répartition de leurs responsabilités. Cette organisation a pour objectif affiché de garantir un contrôle efficace des systèmes d'IA par les administrations et agences sectorielles.

La CNIL sera notamment compétente pour les pratiques interdites liées à l'identification biométrique à distance en temps réel à des fins répressives, ainsi que pour les systèmes à haut risque utilisés dans la gestion de la main-d'œuvre. Les systèmes déployés dans les infrastructures critiques relèveront des Hauts fonctionnaires de défense et de sécurité des ministères concernés.

La DGCCRF est désignée comme point de contact unique pour la coordination opérationnelle des autorités de surveillance du marché, conformément à l'article 70(2) du RIA. La Direction générale des entreprises (DGE) assurera la coordination stratégique. En appui, l'ANSSI et le Pôle d'Expertise de la Régulation Numérique (PEReN) fourniront un socle de compétences techniques mutualisées pour le contrôle de conformité des systèmes d'IA.

Cette répartition des compétences doit encore être validée par le Parlement dans le cadre d'un projet de loi, marquant une étape importante dans la mise en œuvre du cadre européen pour l'intelligence artificielle.

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