Digital Omnibus de l'UE : simplifier le droit numérique sans affaiblir la protection des données ? Analyse des avis conjoints du CEPD et EDPS

Anne-Catherine Berg, le 24 février 2026

Après avoir multiplié les textes réglementaires, du RGPD à l'AI Act, l'UE cherche désormais à les rendre plus cohérents, lisibles et opérationnels afin de simplifier la mise en conformité, réduire la charge administrative et renforcer la compétitivité européenne. Retour sur les deux avis rendus par le CEPD et EDPS.

Avis conjoint 2/2026 du CEPD et du CEPD sur la proposition de règlement concernant la simplification du cadre législatif numérique (Digital Omnibus)

Avis conjoint 1/2026 du CEPD et du CEPD sur la proposition de règlement concernant la simplification de la mise en œuvre de règles harmonisées en matière d'intelligence artificielle (Omnibus numérique sur l'IA)

Introduction

Le 19 novembre 2025, la Commission européenne a présenté le paquet « Digital Omnibus », une initiative visant à rationaliser un cadre réglementaire numérique devenu particulièrement dense et complexe après une décennie d'adoption de textes tels que le RGPD, la directive ePrivacy, le Data Act, le Data Governance Act, NIS 2 et l'AI Act. L'objectif n'est plus d'introduire de nouvelles obligations, mais de rendre les règles existantes plus lisibles, cohérentes et opérationnelles afin de faciliter la conformité, renforcer la sécurité juridique et soutenir la compétitivité européenne.

Deux propositions sont actuellement examinées au niveau de l'UE : un règlement de simplification du cadre législatif numérique « Digital Omnibus » (portant notamment sur le RGPD et l'acquis en matière de données) et un texte spécifique relatif à la simplification de la mise en œuvre de l'AI Act « Digital Omnibus AI ». Leur adoption est envisagée en 2026 pour une entrée en vigueur probable en 2027–2028.

Présentée comme un exercice technique de simplification, l'initiative soulève toutefois une question plus fondamentale : s'agit-il d'un simple ajustement technique visant à faciliter la

conformité ou d'une évolution plus substantielle susceptible de modifier l'équilibre entre innovation et protection des droits fondamentaux au cœur du modèle européen ? Les réactions sont partagées entre rationalisation bienvenue (cf. Peter Craddock, Rendre le RGPD réaliste ? Les autorités ne le souhaitent qu'à moitié ; Béatrice Ericson, Sid Hollman, Alberto di Felice, Digital omnibus : a first step and what must come next, now), et risque d'affaiblissement des garanties existantes en matière de protection des données (cf. NOYB, Digital Omnibus Report V2 : Analysis of Select GDPR and ePrivacy Proposals by the Commission ; NOYB, Digital Omnibus : EU DPAs reject many proposed changes to the GDPR).

Dans ce contexte, le Comité européen de la protection des données (CEPD) et le Contrôleur européen de la protection des données (EDPS) ont adopté deux avis conjoints (l'avis 1/2026 du 20 janvier 2026 relatif au Digital Omnibus AI, puis l'avis 2/2026 du 10 février 2026 consacré au Digital Omnibus), qui permettent d'apprécier la portée réelle de l'initiative et les limites de la simplification au regard de la protection des données personnelles. En raison de la portée extraterritoriale du droit numérique européen, notamment du RGPD, du Data Act et, à terme, de l'AI Act, ces évolutions concernent également de nombreuses organisations en Suisse (cf. Flavio Caci, The Digital Omnibus debate, in : MAG, LegalCommunityCH, Switzerland on the rise : moves and appointments in 2025, p. 40, disponible : ici.).

Partie I. Avis conjoint 2/2026 du CEPD et de l'EDPS sur le Digital Omnibus

L'avis conjoint du CEPD et de l'EDPS examine principalement les modifications proposées du RGPD, de la directive ePrivacy et, plus largement, de l'acquis européen en matière de données. Si les autorités soutiennent l'objectif général de clarification et certaines mesures de simplification, elles s'opposent fermement à toute modification susceptible de réduire la portée matérielle du RGPD ou d'affaiblir le niveau de protection des données à caractère personnel.

1. **Les lignes rouges : définition des données à caractère personnel et pseudonymisation**

La principale critique concerne la modification proposée de la définition des données à caractère personnel. La Commission introduit une approche dite « relative » : une information ne constituerait une donnée personnelle que pour l'entité disposant raisonnablement des moyens d'identifier la personne concernée. La même information pourrait donc être qualifiée de donnée non personnelle pour un autre acteur ne disposant pas de ces moyens.

Le CEPD et l'EDPS estiment que cette approche dépasse la jurisprudence récente de la CJUE

(cf. C-413/23, commentaire disponible : swissprivacy.law/385/) et va bien au-delà d'un ajustement technique. Elle risquerait de restreindre substantiellement la notion de donnée à caractère personnel, et par conséquent le champ d'application matériel du RGPD, tout en introduisant une forte incertitude juridique notamment dans les chaînes d'acteurs, les environnements cloud et l'écosystème de l'IA.

Ils s'opposent également à ce que la Commission puisse, par acte d'exécution, déterminer à quelles conditions des données pseudonymisées sortiraient du champ du RGPD. Une telle décision, soulignent-ils, relève des autorités de contrôle et des juridictions, puisqu'elle touche directement à la portée du règlement lui-même.

Pour les organisations en Suisse, l'enjeu est significatif : la qualification de données à caractère personnel conditionne non seulement l'application extraterritoriale du RGPD, mais influence également l'interprétation de la notion de « données personnelles » en droit suisse, dont la compréhension demeure étroitement liée à la jurisprudence européenne.

2. **Mesures de simplification globalement soutenues**

Recherche scientifique : Le CEPD et l'EDPS saluent l'introduction d'une définition harmonisée de la recherche scientifique. Dans ce cadre, ils admettent que le traitement puisse, sous réserve du respect de l'ensemble des exigences du RGPD, reposer sur l'intérêt légitime, être considéré comme compatible avec la finalité initiale sans application de l'art. 6 par. 4 RGPD et bénéficier d'une dérogation limitée à l'obligation d'information. Ils insistent toutefois sur la nécessité d'un encadrement strict : la recherche doit suivre une méthodologie scientifique indépendante, produire des résultats vérifiables et transparents, contribuer à l'avancement des connaissances et respecter des standards éthiques. À l'inverse, de simples activités d'innovation ou de développement de produits ne sauraient automatiquement être qualifiées de recherche scientifique, ce qui en limite la portée pratique pour certaines organisations.

Authentification biométrique : Une nouvelle exception autorisant le traitement de catégories particulières de données à des fins d'authentification biométrique est soutenue, à condition que les données restent sous le contrôle exclusif de la personne concernée (par exemple stockage sur un badge ou un appareil personnel détenu par l'utilisateur).

Notifications de violations et analyses d'impact : Le CEPD et l'EDPS soutiennent plusieurs mesures de simplification : l'harmonisation des modèles de notification et l'établissement d'une liste commune des situations nécessitant une analyse d'impact relative à la protection des données, pour autant que son élaboration relève du CEPD plutôt que de la

Commission ; le relèvement du seuil de notification des violations de données au niveau de « risque élevé » ; l'allongement du délai de notification de 72 à 96 heures ; ainsi que la mise en place d'un guichet européen unique pour la déclaration des incidents de sécurité, couvrant notamment le RGPD, NIS 2, DORA et eIDAS.

3. **Points nécessitant des clarifications**

Intelligence artificielle

Le CEPD et l'EDPS rappellent que le RGPD permet déjà, dans certaines situations, de fonder le développement et l'exploitation de systèmes ou modèles d'IA sur l'intérêt légitime (art. 6 par. 1 let. f RGPD). Cette base juridique n'est toutefois admissible qu'au terme d'une évaluation au cas par cas, rigoureuse et documentée, comprenant le test en trois étapes (nécessité, mise en balance des intérêts et garanties appropriées), assortie d'une transparence renforcée et d'un droit d'opposition effectif pour les personnes concernées. Dans cette perspective, l'introduction d'une nouvelle base juridique spécifique dans le RGPD n'apparaît pas nécessaire : l'enjeu réside plutôt dans l'application exigeante du cadre existant.

Concernant le traitement « incident et résiduel » de données sensibles dans l'IA, les autorités admettent le principe d'une dérogation, mais uniquement comme solution de dernier recours. Elle ne peut viser que des traitements réellement involontaires et inévitables lors de l'entraînement ou du test d'un système, à condition que la suppression des données soit impossible ou disproportionnée et que des garanties techniques et organisationnelles couvrent l'ensemble du cycle de vie de l'IA. Cette exception ne saurait en revanche justifier un traitement nécessaire au fonctionnement du modèle ni s'étendre aux données sensibles fournies par les utilisateurs, notamment via des prompts.

Droits des personnes

Le CEPD et l'EDPS approuvent l'objectif de mieux encadrer les demandes d'accès manifestement abusives, mais à une condition essentielle : une demande ne peut être qualifiée d'abusive qu'en présence d'une intention abusive démontrable (par exemple la volonté de nuire au responsable du traitement), et non en raison du but poursuivi par la personne concernée. Ils soulignent en outre que les demandes larges ne doivent pas être automatiquement considérées comme excessives et qu'un refus doit reposer sur une appréciation objective et dûment documentée, la personne devant, le cas échéant, pouvoir préciser sa demande.

Les autorités soutiennent également une simplification des obligations d'information, notamment pour les PME, à condition qu'elle reste strictement encadrée et ne prive pas les personnes de la possibilité d'obtenir les informations pertinentes sur l'utilisation de leurs données. Enfin, elles insistent sur le maintien de l'art. 22 RGPD tel qu'interprété par la CJUE : une interdiction de principe, assortie d'exceptions strictes. Le texte doit donc conserver cette logique afin d'éviter une extension excessive du recours aux décisions automatisées.

4. **ePrivacy – protection des équipements terminaux (cookies)**

Le Digital Omnibus pourrait constituer la réforme la plus structurante des règles sur les cookies depuis l'entrée en application du RGPD. Le projet prévoit d'intégrer au RGPD les règles de la directive ePrivacy relatives à l'accès et au stockage d'informations sur les terminaux des utilisateurs (les dispositions sur les cookies) et d'introduire des mécanismes de gestion du consentement automatisés, fondés sur des signaux de préférences lisibles par machine transmis par les navigateurs, systèmes d'exploitation ou applications. À terme, ces mécanismes pourraient remplacer les bannières cookies traditionnelles en permettant à l'utilisateur d'exprimer ses choix une seule fois.

Si le CEPD et l'EDPS soutiennent l'objectif de réduction de la « fatigue du consentement aux cookies » et la recherche d'une solution technique plus efficace, ils soulignent toutefois un risque important d'insécurité juridique : la coexistence de deux régimes distincts selon que les données sont personnelles (RGPD) ou non personnelles (ePrivacy). Ce qui pourrait rendre difficile l'identification du cadre applicable, alors même que les traceurs combinent fréquemment les deux types d'informations. Les autorités rappellent également que la protection des terminaux relève non seulement du droit à la protection des données, mais aussi du respect de la vie privée et de la confidentialité des communications.

Les nouvelles exceptions au consentement, notamment pour la mesure d'audience ou la sécurité, sont admises, mais uniquement si elles restent strictement limitées au nécessaire. La mesure d'audience devrait reposer sur des données agrégées et anonymes, sans combinaison avec d'autres services ni partage avec des tiers, tandis que les mises à jour de sécurité ne pourraient être installées sans consentement qu'à condition de ne pas modifier les fonctionnalités et d'informer l'utilisateur. Dans la même logique, les autorités encouragent le développement de la publicité contextuelle, moins intrusive que la publicité comportementale.

Elles soutiennent en revanche l'introduction de signaux de consentement automatisés, à condition qu'ils reposent sur des standards harmonisés, ne conduisent pas à un consente-

ment par défaut et s'imposent à l'ensemble des acteurs (sites, fournisseurs d'applications, navigateurs et systèmes d'exploitation).

Pour les entreprises suisses, plateformes, éditeurs, fournisseurs SaaS, fintech ou acteurs adtech, les conséquences seraient immédiates : les outils de gestion du consentement, les traceurs, les pratiques d'analytics et certains modèles publicitaires devront être repensés pour les utilisateurs situés dans l'UE. En pratique, la proposition ne se limite donc pas à supprimer les bannières cookies : elle annonce une transformation technique et organisationnelle de la gestion du suivi et de la publicité en ligne.

5. **Data acquis**

De manière générale, le CEPD et l'EDPS soutiennent la consolidation de « l'acquis en matière de données » au sein d'un instrument unique et cohérent sur le partage et l'utilisation des données, notamment par l'intégration, dans le Data Act, des règles issues du Data Governance Act, du règlement sur la libre circulation des données non personnelles et de la directive Open Data tout en abrogeant ces textes. L'objectif est de réduire les chevauchements normatifs et d'accroître la sécurité juridique. Les autorités rappellent toutefois que la simplification ne doit ni ouvrir la voie à l'accès à des données personnelles non pseudonymisées en situation d'urgence, ni affaiblir les mécanismes de confiance entourant l'intermédiation et l'altruisme des données. Elle doit également s'accompagner de clarifications quant aux responsabilités respectives des acteurs (mesures techniques et organisationnelles, supervision, coopération et articulation avec le RGPD).

En pratique, toute entreprise suisse qui met sur le marché européen un produit connecté, propose un service en ligne ou exploite des données générées dans l'UE pourra être concernée. Les organisations devront dès lors revoir leurs cadres contractuels (CGV, SLA, accords de partage de données), instaurer une gouvernance des données réellement opérationnelle et faire évoluer leurs systèmes techniques afin de garantir l'accès et la portabilité des données, ainsi que leur transmission à des tiers désignés par les utilisateurs et, dans certaines circonstances, aux autorités publiques.

Partie II. Avis 1/2026 conjoint CEPD/EDPS sur le Digital Omnibus AI

Dans l'ensemble, le CEPD et l'EDPS soutiennent la proposition « Digital Omnibus AI », destinée à faciliter l'application pratique de l'AI Act par des simplifications ciblées et une réduction des charges administratives. Ils annoncent également l'élaboration de lignes directrices conjointes avec la Commission européenne afin de préciser l'articulation entre le RGPD et l'AI

Act.

Ils rappellent toutefois que la simplification ne doit ni affaiblir la protection des droits fondamentaux, en particulier des données personnelles, ni accroître l'insécurité juridique. Leur avis identifie ainsi plusieurs points nécessitant des clarifications et des garanties supplémentaires pour concilier innovation et niveau élevé de protection.

1. **Traitement des catégories particulières de données pour la détection et la correction des biais**

La proposition de la Commission élargit la dérogation permettant le traitement de catégories particulières de données à caractère personnel dites sensibles à des fins de détection et de correction des biais : elle s'appliquerait désormais à l'ensemble des systèmes et modèles d'IA et non plus seulement aux systèmes « à haut risque », et couvrirait également les déployeurs (utilisateurs). Le CEPD et l'EDPS reconnaissent que l'identification des biais peut, dans certains cas, nécessiter l'usage de données sensibles afin d'éviter des discriminations. Ils rappellent toutefois que ce type de traitement doit rester strictement encadré. Ils demandent en particulier de rétablir l'exigence de « stricte nécessité », de limiter cette possibilité aux situations où le risque d'atteinte aux droits fondamentaux est suffisamment sérieux, et de préciser clairement l'articulation avec les art. 6 et 9 RGPD afin d'éviter toute insécurité juridique.

2. **Enregistrement et documentation**

La Commission propose de supprimer l'obligation d'enregistrement lorsqu'un fournisseur considère qu'un système d'IA relevant de l'annexe III de l'AI Act ne présente finalement pas un niveau de risque « élevé ». Le CEPD et l'EDPS s'y opposent : l'inscription dans la base européenne constitue, selon eux, un élément central de transparence et de traçabilité, utile tant pour le public et les utilisateurs que pour les autorités de contrôle avant la mise sur le marché. Sa suppression affaiblirait la responsabilité des fournisseurs et créerait une incitation à requalifier abusivement certains systèmes afin d'échapper aux exigences applicables aux systèmes à haut risque.

Enfin, elles mettent en garde contre un allègement des obligations fondé uniquement sur la taille de l'entreprise (PME), la capacité de nuisance d'un système d'IA dépendant davantage de ses caractéristiques et de sa diffusion que du nombre d'employés du fournisseur.

3. **Bacs à sable réglementaires IA (AI sandboxes)**

Le CEPD et l'EDPS soutiennent la mise en place de bacs à sable réglementaires au niveau de l'UE, en complément des dispositifs nationaux, afin de favoriser l'innovation, notamment pour les PME mais sous réserve de plusieurs garanties : l'implication effective des autorités de protection des données, la clarification de leur compétence et de l'articulation avec les mécanismes de coopération du RGPD, l'attribution d'un rôle consultatif explicite au CEPD.

4. **Supervision par le Bureau européen de l'IA (AI Office)**

L'extension de la compétence exclusive de l'AI Office aux systèmes intégrés dans les très grandes plateformes en ligne et moteurs de recherche (VLOP/VLOSE) au sens du DSA peut renforcer la cohérence de la supervision au niveau européen. Le CEPD et l'EDPS soulignent toutefois plusieurs points de vigilance : cette centralisation ne doit ni entraver l'indépendance ni limiter la capacité d'intervention des autorités nationales si l'AI Office n'agit pas. Ils insistent également sur la nécessité d'une coopération étroite avec les autorités de protection des données lorsque des risques pour la vie privée ou les données personnelles sont en cause.

5. **Coopération des autorités**

Le CEPD et l'EDPS soutiennent le renforcement de la coopération entre les autorités de protection des droits fondamentaux (FRABs) et les autorités de surveillance du marché (MSAs), notamment par la création d'un point de contact centralisé pouvant simplifier les démarches des opérateurs, sous réserve du respect des conditions suivantes : clarification précise des rôles respectifs des autorités, limitation des MSAs à une fonction de relais administratif, préservation de l'indépendance et des pouvoirs propres des autorités de protection des données ainsi qu'une organisation claire et rapide des échanges d'informations, y compris en situation transfrontière, dont les modalités d'assistance doivent être explicitement définies.

6. **AI literacy**

Le CEPD et l'EDPS s'opposent à la transformation de cette obligation en simple mesure d' encouragement. Selon eux, la formation à l'IA constitue un élément clé : elle permet de comprendre les concepts, risques et bénéfices de la technologie, de renforcer la vigilance éthique et de garantir la protection des droits fondamentaux, en particulier la protection des données. Ils recommandent donc de maintenir une responsabilité directe des fournisseurs et déployeurs, les initiatives publiques devant seulement accompagner et soutenir cet effort, et non s'y substituer.

7. **Calendrier d'application des règles relatives aux systèmes d'IA à haut risque**

Le calendrier initial de l'AI Act prévoit l'application des règles pour les systèmes d'IA à haut risque au 2 août 2026 (Annexe III) et au 2 août 2027 (Annexe I). La proposition reporte ces échéances : elles s'appliqueraient 6 à 12 mois après la mise à disposition des outils de conformité, au plus tard en décembre 2027 et août 2028. Le CEPD et l'EDPS reconnaissent les difficultés pratiques de mise en œuvre, mais mettent en garde contre un report du calendrier initial : il retarderait l'effectivité des garanties prévues par l'AI Act, augmenterait le nombre de systèmes à haut risque opérant sans encadrement complet et créerait une incertitude juridique accrue. Ils invitent dès lors à limiter autant que possible les délais et à maintenir, lorsque cela est faisable, certaines obligations, en particulier celles relatives à la transparence.

Conclusion

A la lumière des avis conjoints du CEPD et de l'EDPS, le Digital Omnibus s'apparente moins à une simple simplification technique qu'à un ajustement structurant de la régulation numérique européenne, visant à mieux articuler le RGPD, la directive ePrivacy, le Data Act et l'AI Act dans un cadre réglementaire cohérence et opérationnel. Les autorités en fixent toutefois la limite essentielle : la simplification ne doit ni réduire la portée matérielle du RGPD ni affaiblir le niveau de la protection des données à caractère personnel.

Pour les entreprises suisses exerçant des activités ou ciblant des clients dans l'UE, l'impact sera direct en raison de la portée extraterritoriale, notamment, du RGPD et de l'AI Act. L'accès au marché européen dépendra désormais du respect combiné de la réglementation de l'UE relative à la protection des données, au partage des données et à la gouvernance de l'intelligence artificielle.

Le Digital Omnibus demeure à ce stade une proposition. Il reste à voir dans quelle mesure les co-législateurs suivront les recommandations du CEPD et de l'EDPS. Dans l'attente de l'issue du processus législatif européen, la stratégie la plus prudente consiste à poursuivre la mise en conformité sur la base des textes en vigueur, en particulier le RGPD et l'AI Act, afin d'anticiper les exigences futures, quelle que soit l'évolution des négociations. Certains observateurs suisses (cf. Flavio Caci, The Digital Omnibus debate, in : MAG, LegalCommunityCH, Switzerland on the rise : moves and appointments in 2025, p. 40, disponible : ici) relèvent toutefois que plusieurs modifications proposées du RGPD rapprocheraient le droit de l'UE du régime suisse issu de la loi fédérale révisée sur la protection des données, sans créer de tensions majeures.

Proposition de citation : Anne-Catherine BERG, Digital Omnibus de l'UE : simplifier le droit numérique sans affaiblir la protection des données ? Analyse des avis conjoints du CEPD et EDPS, 24 février 2026 *in* www.swissprivacy.law/396