_swissprivacy.law

Protection des données dans la proposition de règlement sur la cybersécurité 2

Pauline Meyer, le 14 avril 2026

Le 18 mars 2026, le Comité européen de la protection des données et le Contrôleur européen de la protection des données ont publié leur opinion jointe sur la protection des données dans le projet de CSA2 et les modifications proposées à la directive NIS2.

EDPB-EDPS Joint Opinion [4/2026]

CSA2 et modifications de NIS2

La mise en œuvre du Règlement sur la cybersécurité (Cybersecurity Act, CSA), en vigueur depuis 2019, est confrontée à plusieurs obstacles : un décalage entre la politique de cybersécurité de l'UE et les besoins des parties prenantes dans un environnement où les cybermenaces sont toujours plus hostiles et complexes, des freins dans la mise en œuvre du cadre européen de certification en matière de cybersécurité, la complexité et la diversité des politiques nationales de cybersécurité influençant la posture de l'UE et les risques croissants pour la sécurité des chaînes d'approvisionnement dans le domaine des technologies de l'information et des communications (TIC).

Par conséquent, une proposition de CSA2 (P-CSA2) prévoit de renforcer le rôle opérationnel de l'Agence européenne pour la cybersécurité (ENISA) et la coopération en matière de cybersécurité dans l'UE. Le projet vise également une amélioration réglementaire pour le cadre européen de certification en matière de cybersécurité, et crée un cadre pour les risques non techniques liés à la chaîne d'approvisionnement des TIC.

Le P-CSA2 s'accompagne d'une proposition de modifications ciblées de la Directive NIS2 (P-NIS2). Les modifications consistent notamment en des clarifications du champ d'application de la directive, en des améliorations du lien entre NIS2 et le cadre européen de schémas de certification de cybersécurité, en la prise en compte de la cryptographie post-quantique dans les politiques d'États-membres ou en l'introduction d'un système harmonisé de collecte de données sur les attaques par rançongiciels.

Opinion du CEPD et de l'EDPS

Dans l'ensemble, le Comité européen de la protection des données (CEPD) et le Contrôleur européen de la protection des données (EDPS) accueillent favorablement le P-CSA2.

En particulier, les deux entités soutiennent les objectifs généraux de renforcement du rôle, du soutien et de la coopération d'ENISA, la simplification de l'adoption de schémas de certification et le traitement dans le règlement des risques non techniques relatifs aux chaînes d'approvisionnement critiques dans le domaine des TIC.

Déjà exprimé dans leur avis sur la proposition de règlement omnibus numérique (pour plus d'information, voir : swissprivacy.law/396/), le CEPD et l'EDPBS rappellent leur soutien à la création, par ENISA, d'un guichet unique pour le signalement de cyberincidents (art. 15 P-CSA2 et proposition d'art. 23bis NIS2 dans la proposition de règlement omnibus numérique), mais également selon d'autres réglementations, principalement le RGPD.

Dans le cadre des modifications de la Directive NIS2, le CEPD et l'EDPS saluent en particulier l'adoption de mécanismes permettant de faciliter la conformité avec ses exigences et la désignation des fournisseurs de portefeuilles européens d'identité numérique comme entités essentielles.

L'avis joint reflète également des aspects questionnés par les autorités. Par exemple, elles soulèvent la nécessité de préciser quels types d'informations sont amenés à être traités par ENISA dans ses tâches de « central hub » en vertu des art. 10 et 11 P-CSA2. En particulier, les dispositions du P-CSA2 devraient préciser si ces tâches d'ENISA requièrent le traitement de données personnelles d'une ampleur substantielle (à l'instar d'adresse IP, logs d'utilisations ou détails de comptes compromis).

Si, au contraire, ENISA traite principalement des données agrégées à caractère non personnel, cela devrait être précisé, au moins par le biais d'un considérant. Dans tous les cas, seuls les détails techniques peuvent être écartés du règlement et laissés à l'autonomie administrative du conseil d'administration d'ENISA (art. 66(2) P-CSA2).

En outre, l'art. 19(2) P-CSA2 propose l'élaboration par ENISA d'un cadre européen pour les compétences en matière de cybersécurité (ECSF) établissant une vision commune aux exigences liées aux métiers de la cybersécurité. Le CEPD et l'EDPS estiment que le cadre devrait aussi inclure un profil « cybersécurité pour les généralistes » qui couvrirait les compétences minimales nécessaires que tout résident de l'UE en âge de travailler devrait posséder

pour interagir en toute sécurité au sein d'un marché numérique (devant exister en parallèle du cadre DigComp 3.0). En outre, l'ECSF devrait inclure un module consacré à la conformité des mesures de cybersécurité avec la protection des données.

Le CEPD et l'EDPS considèrent que des synergies entre les schémas de certification de cybersécurité et de protection des données existent et que le lien entre la portée de l'art. 80(1)(w) P-CSA2 et la certification selon RGPD (art. 42 s. RGPD) devrait être clarifié. Ils recommandent la consultation du CEPD par ENISA avant l'adoption d'un schéma de certification afin d'assurer un certain niveau de cohérence.

Finalement, et bien que le CEPD et l'EDPS saluent la communication d'informations relatives aux rançongiciels prévue à l'art. 23(12) et (13) P-NIS2, ils estiment que, compte tenu du caractère sensible des données communiquées, les garanties de protection des données applicables devraient être précisées dans les actes d'exécution adoptés par la Commission en vertu de l'actuel art. 23(11) P-NIS2 et que l'EDPS devrait être consulté à ce sujet.

Remarques

Les P-CSA2 et P-NIS2 interviennent dans un contexte de changements au sein des réglementations technologiques européennes, peu de temps après la proposition de règlement omnibus numérique. Dans ces approches de simplification et harmonisation, nous pouvons particulièrement saluer d'une part l'adoption d'une section du P-CSA2 dédiée à réduire les dépendances critiques et les risques liés aux chaînes d'approvisionnement critiques dans le domaine des TIC provenant de fournisseurs à haut risque.

D'autre part, la conformité avec les exigences, principalement de NIS2, devrait être facilitée par deux mécanismes. L'introduction du guichet unique d'ENISA déjà formulée dans le P-NIS2 devrait contribuer à simplifier la mise en œuvre d'obligations de signalement. En outre, l'amélioration du cadre européen de certification de cybersécurité et de son interaction avec la Directive NIS2 devrait permettre une harmonisation des pratiques, en particulier dans les responsabilités liées aux chaînes d'approvisionnement (art. 21 NIS2).

Proposition de citation : Pauline Meyer, Protection des données dans la proposition de règlement sur la cybersécurité 2, 14 avril 2026 *in* www.swissprivacy.law/405