



European
Data Protection
Board



Avis conjoint du comité européen de la protection des données et du Contrôleur européen de la protection des données [4/2026]

sur la proposition de règlement sur la
cybersécurité 2
et la proposition de modification de la
directive SRI 2

Adopté le 18 mars 2026

Table des matières

1	Contexte.....	5
2	Remarques générales.....	6
3	Soutien de l'ENISA à la mise en œuvre de la politique et du droit de l'Union et coopération avec d'autres entités de l'Union	7
4	Coopération opérationnelle, connaissance commune de la situation en matière de cybersécurité et protection des données à caractère personnel.....	8
5	Point d'entrée unique pour la notification des incidents (article 15 de la proposition CSA2)	10
6	Cadre européen des compétences en matière de cybersécurité (ECSF) (article 19 de la proposition CSA2)	11
7	Cadre européen de certification de cybersécurité (titre III)	13
8	Cadre de confiance pour la chaîne d'approvisionnement des TIC (titre IV).....	15
9	Entités essentielles supplémentaires au titre de la proposition de modification de la directive SRI 2	15
10	Collecte de données sur les attaques par rançongiciel	16

Résumé

Le 20 janvier 2026, la Commission européenne a publié une proposition de règlement relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2), ainsi qu'une proposition de directive modifiant la directive (UE) 2022/2555 en ce qui concerne les mesures de simplification et l'alignement sur la [proposition de règlement sur la cybersécurité 2]. Le 21 janvier 2026, la Commission a officiellement consulté le comité européen de la protection des données (ci-après le «comité») et le Contrôleur européen de la protection des données (ci-après le «Contrôleur») conformément à l'article 42, paragraphe 2, du règlement (UE) 2018/1725.

Le comité et le Contrôleur rappellent que la relation entre la protection des données et la cybersécurité est bidirectionnelle. D'une part, la cybersécurité sert la protection des données à caractère personnel en limitant les risques d'accès non désiré, de modification ou d'indisponibilité de ces données. D'autre part, certaines mesures de cybersécurité peuvent interférer avec les droits et libertés des personnes, en particulier les droits au respect de la vie privée et à la protection des données. Par conséquent, si l'efficacité est une priorité importante pour les mesures de cybersécurité, il convient de tenir compte de la nécessité et de la proportionnalité.

Le comité et le Contrôleur soutiennent l'objectif général des propositions consistant à renforcer le rôle de l'ENISA et à faciliter l'adoption de la certification de cybersécurité, sous réserve des recommandations spécifiques formulées dans le présent avis conjoint. Ils se félicitent également de l'objectif visant à mettre en place, dans la directive (UE) 2022/2555, des mécanismes et des conditions destinés à faciliter le respect des exigences en matière de cybersécurité et, ainsi, de rendre leur mise en œuvre plus cohérente et plus efficace, ainsi que de l'objectif visant à mieux faire face aux différents risques pesant sur les chaînes d'approvisionnement des TIC, y compris les risques non techniques. Le comité et le Contrôleur soutiennent également fermement l'objectif de la mise en place d'un point d'entrée unique pour la notification des violations de données à caractère personnel, car cela réduirait la charge administrative pour les organisations sans affecter le niveau de protection des personnes concernées.

Le comité et le Contrôleur se félicitent également que la proposition de règlement sur la cybersécurité 2 apporte des précisions supplémentaires sur les modalités selon lesquelles l'ENISA apporte son soutien aux différentes parties prenantes, et recommandent d'ajouter également le Contrôleur parmi les entités pouvant solliciter un avis de l'ENISA. Le comité et le Contrôleur soutiennent fermement l'idée que cet avis ne soit rendu qu'à la suite d'une demande, afin de garantir une coordination claire et une répartition précise des responsabilités.

En ce qui concerne la coopération entre l'ENISA et d'autres entités de l'Union en général, le comité et le Contrôleur se félicitent des synergies que cette coopération peut permettre, conformément à leurs missions et mandats respectifs. Ils recommandent d'ajouter également une référence explicite au Contrôleur en tant qu'organe de l'Union, avec lequel l'ENISA coopérerait.

Le comité et le Contrôleur estiment que si les futures missions de l'ENISA en tant que plateforme d'information nécessitent un traitement substantiel de données à caractère personnel, cela devrait être explicitement énoncé dans les dispositions de l'acte de base régissant les missions respectives, y compris les éléments essentiels de tout traitement à grande échelle et les garanties appropriées. À l'inverse, si l'objectif est de permettre à l'ENISA de collecter et de traiter principalement des données à caractère non personnel agrégées, cela devrait également être précisé.

Le comité et le Contrôleur rappellent qu'en principe, seuls les détails très techniques (pratiques) liés au traitement des données à caractère personnel devraient être décidés dans le cadre de l'autonomie administrative de l'organe de l'Union concerné (en l'occurrence, le conseil d'administration d'une agence décentralisée). En outre, le comité et le Contrôleur recommandent de prévoir, à l'article 66 de la proposition de règlement sur la cybersécurité 2, une consultation préalable du Contrôleur avant l'adoption de ces règles.

En ce qui concerne le cadre européen des compétences en matière de cybersécurité (ECSF), le comité et le Contrôleur recommandent aux colégislateurs de modifier l'article 19, paragraphe 2, de la proposition de règlement sur la cybersécurité 2 afin que l'ECSF ne se limite pas exclusivement aux «professionnels de la cybersécurité», mais comprenne également des profils pour la main-d'œuvre en général.

En ce qui concerne le cadre européen de certification de cybersécurité, le comité et le Contrôleur recommandent de clarifier davantage le champ d'application de l'article 80, paragraphe 1, point w), de la proposition de règlement sur la cybersécurité 2 et la relation avec la certification au titre du règlement général sur la protection des données (RGPD). En outre, le comité et le Contrôleur recommandent d'exiger de l'ENISA qu'elle consulte le comité avant d'adopter un système de certification au titre de l'article 80, paragraphe 1, point w), de la proposition de règlement sur la cybersécurité 2 afin de garantir la cohérence.

Le comité et le Contrôleur soulignent l'importance de tenir compte non seulement de l'efficacité des mesures de cybersécurité, mais aussi de leur nécessité et de leur proportionnalité. Le comité et le Contrôleur recommandent de préciser que les systèmes de certification devraient, dans la mesure du possible, tenir compte des contrôles de sécurité susceptibles de contribuer à démontrer le respect des exigences du RGPD, en particulier lorsque les systèmes s'appliquent à des produits TIC, à des services TIC, à des processus TIC et à des services de sécurité gérés susceptibles d'être utilisés dans des opérations de traitement de données.

Le comité et le Contrôleur se félicitent en outre de la mesure proposée visant à garantir un cadre de confiance pour la chaîne d'approvisionnement des TIC et à faire face aux risques non techniques dans les secteurs hautement critiques.

En ce qui concerne la proposition modifiant la directive SRI 2, le comité et le Contrôleur se félicitent de la désignation des portefeuilles européens d'identité numérique et des fournisseurs de portefeuilles européens d'identité numérique pour les entreprises en tant qu'«entités essentielles», et soutiennent pleinement l'objectif crucial consistant à prévenir de futures attaques par rançongiciel ainsi qu'à perturber et à démanteler les organisations criminelles qui en sont à l'origine.

Le comité européen de la protection des données et le Contrôleur européen de la protection des données

Vu l'article 42, paragraphe 2, du règlement (UE) 2018/1725 du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE,

Ont adopté l'avis conjoint suivant (ci-après l'«avis»)

1 CONTEXTE

1. Le 20 janvier 2026, la Commission européenne (ci-après la «Commission») a publié une proposition de règlement relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2)¹ et une proposition de directive modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur la [proposition de règlement sur la cybersécurité 2]² (ci-après la «proposition CSA2», la «proposition de modification de la directive SRI 2» et, conjointement, les «propositions»). Le 21 janvier 2026, la Commission a officiellement consulté le comité et le Contrôleur conformément à l'article 42, paragraphe 2, du règlement (UE) 2018/1725 (ci-après le «RPDUE»)³.
2. La proposition CSA2 vise à remplacer l'actuel règlement sur la cybersécurité⁴ afin 1) de renforcer le rôle de l'ENISA en mettant l'accent sur les besoins des parties prenantes dans un paysage de menaces de plus en plus hostile, 2) de relancer la mise en œuvre du cadre européen de certification de cybersécurité, 3) de réduire la complexité et la diversité des politiques liées à la cybersécurité, et 4) de mieux faire face aux risques pour la sécurité de la chaîne d'approvisionnement des TIC⁵.
3. La proposition de modification de la directive SRI 2 se concentre en particulier sur le troisième objectif, en apportant des clarifications et en facilitant la mise en conformité des entités réglementées⁶.

¹ COM(2026) 11 final.

² COM(2026) 13 final.

³ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

⁴ Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15-69, ELI:) <http://data.europa.eu/eli/reg/2019/881/oj>, tel que modifié par le règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024 modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés (JO L, 2025/37, 15.1.2025, ELI:) <http://data.europa.eu/eli/reg/2025/37/oj>.

⁵ Exposé des motifs, COM(2026) 11 final, p. 1.

⁶ COM(2026) 13 final.

4. L'objectif du présent avis conjoint est d'examiner les aspects pertinents des propositions qui revêtent une importance particulière pour la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel.

2 REMARQUES GÉNÉRALES

5. La proposition CSA2 vise à élargir le mandat de l'ENISA et à le rendre plus opérationnel. Le comité et le Contrôleur soutiennent le renforcement du rôle de l'ENISA et l'objectif de faciliter l'adoption de la certification de cybersécurité, sous réserve des recommandations spécifiques formulées ci-dessous.
6. Le comité et le Contrôleur se félicitent également de l'objectif visant à mettre en place, dans la directive (UE) 2022/2555⁷ (ci-après la «directive SRI 2»), des mécanismes et des conditions destinés à faciliter le respect des exigences en matière de cybersécurité et, ainsi, de rendre leur mise en œuvre plus cohérente et plus efficace, ainsi que de l'objectif visant à mieux faire face aux différents risques pesant sur les chaînes d'approvisionnement des TIC, y compris les risques non techniques.
7. Comme déjà indiqué dans leur avis conjoint sur la proposition «omnibus numérique»⁸, le comité et le Contrôleur soutiennent fermement l'objectif de la mise en place d'un point d'entrée unique pour la notification des violations de données à caractère personnel, car cela réduirait la charge administrative pour les organisations sans affecter le niveau de protection des personnes concernées.
8. L'article 5, paragraphe 1, point f), du règlement (UE) 2016/679 (RGPD) fait de la sécurité l'un des grands principes relatifs au traitement des données à caractère personnel. L'article 32 du RGPD définit plus précisément cette obligation, applicable tant aux responsables du traitement qu'aux sous-traitants, de garantir un niveau de sécurité approprié. Ces deux dispositions indiquent clairement que la sécurité du traitement des données à caractère personnel est essentielle au respect de la législation de l'Union en matière de protection des données.
9. La relation entre la protection des données et la cybersécurité est bidirectionnelle. D'une part, la cybersécurité sert la protection des données à caractère personnel en limitant les risques d'accès non désiré, de modification ou d'indisponibilité de ces données. D'autre part, certaines mesures de cybersécurité peuvent interférer avec les droits et libertés des personnes, en particulier les droits au respect de la vie privée et à la protection des données⁹.

⁷ Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

⁸ [Avis conjoint du comité européen de la protection des données et du Contrôleur européen de la protection des données \[2/2026\] concernant la proposition de règlement relative à la simplification du cadre législatif numérique \(train de mesures omnibus sur le numérique\), adopté le 10 février 2026.](#)

⁹ Voir l'[Avis 5/2021 du Contrôleur sur la stratégie de cybersécurité et la directive SRI 2.0](#), 11 mars 2021, points 10 à 11, et l'[Avis 7/2022](#) du Contrôleur sur la proposition de règlement relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union, 17 mai 2022, points 9 à 10, et l'[Avis 2/2024](#) du Contrôleur sur la proposition de règlement modifiant le règlement sur la cybersécurité en ce qui concerne les services de sécurité gérés, 10 janvier 2024, point 5.

10. Le comité et le Contrôleur rappellent que le considérant 49 du RGPD reconnaît que les mesures de cybersécurité impliquant le traitement de données à caractère personnel constituent un intérêt légitime du responsable du traitement concerné, tout en soulignant dans le même temps que les mesures devraient être strictement nécessaires et proportionnées aux fins de garantir la sécurité du réseau et des informations. Par conséquent, les mesures de cybersécurité ne doivent pas seulement être guidées par des considérations d'efficacité, mais doivent également tenir compte de la question de savoir si leur incidence sur les droits fondamentaux reste limitée à ce qui est nécessaire et proportionné.

3 SOUTIEN DE L'ENISA À LA MISE EN ŒUVRE DE LA POLITIQUE ET DU DROIT DE L'UNION ET COOPÉRATION AVEC D'AUTRES ENTITÉS DE L'UNION

11. Conformément à l'article 5, paragraphe 1, de la proposition CSA2, l'ENISA contribue à la mise en œuvre de la politique et du droit de l'Union dans divers domaines, en apportant un soutien aux différentes parties prenantes énumérées audit article.
12. Parmi celles-ci, conformément à l'article 5, paragraphe 1, point h), de la proposition CSA2, l'ENISA fournirait, à la demande du comité européen de la protection des données, des conseils sur la mise en œuvre d'aspects spécifiques de la politique et du droit de l'Union en matière de cybersécurité liés à la protection des données et à la vie privée. Le comité et le Contrôleur notent que l'article 5, paragraphe 1, point h), de la proposition CSA2 n'est pas une disposition entièrement nouvelle. L'article 5, paragraphe 5, point c), de l'actuel règlement sur la cybersécurité prévoit déjà que l'ENISA peut soutenir «les États membres dans la mise en œuvre d'aspects spécifiques en matière de cybersécurité des politiques et du droit de l'Union concernant la protection des données et la vie privée, y compris en fournissant des avis au comité européen de la protection des données à sa demande».
13. Le comité et le Contrôleur se félicitent que la proposition CSA2 apporte des précisions supplémentaires sur les modalités de coopération tout en maintenant les éléments essentiels de l'article 5, paragraphe 5, point c), du règlement sur la cybersécurité. Le nouvel article 5, paragraphe 1, point h), préciserait que le comité, en tant qu'organe de l'Union, est habilité à demander directement l'avis de l'ENISA (sans être lié à la mise en œuvre par les États membres d'aspects spécifiques en matière de cybersécurité des politiques et du droit de l'Union concernant la protection des données et la vie privée).
14. Dans le même temps, le comité et le Contrôleur recommandent d'ajouter également le Contrôleur parmi les entités pouvant solliciter un avis de l'ENISA à l'article 5, paragraphe 1, point h), de la proposition CSA2, compte tenu du rôle de ce dernier en tant qu'autorité de contrôle pour le traitement des données à caractère personnel par les institutions, organes et organismes de l'Union européenne. Permettre au comité et au Contrôleur de s'appuyer sur les compétences techniques de l'ENISA dans le domaine de la cybersécurité peut contribuer à faire en sorte que leurs orientations et décisions dans le domaine de la protection des données s'appuient sur les connaissances les plus récentes en matière de cybersécurité. Il pourrait y avoir plusieurs sujets pour lesquels des conseils et une coopération peuvent être bénéfiques, notamment les normes de cybersécurité et les pratiques opérationnelles, ainsi que l'utilisation des technologies de protection de la vie privée dans le contexte de la cybersécurité.

15. Le comité et le Contrôleur soutiennent fermement que l'avis mentionné à l'article 5, paragraphe 1, point h), de la proposition CSA2 n'est fourni qu'après une demande préalable du comité ou, comme proposé ici, du Contrôleur. En prévoyant que l'ENISA n'agit qu'à la demande du comité ou du Contrôleur, l'article 5, paragraphe 1, point h), garantirait une coordination et une répartition claires des responsabilités¹⁰.
16. Le comité et le Contrôleur notent que l'article 5, paragraphe 1, point h), de la proposition CSA2 semble être une manifestation spécifique d'une obligation de coopération plus générale consacrée à l'article 68 de la proposition CSA2, régissant la coopération de l'ENISA avec d'autres entités de l'Union. Conformément à l'article 68, l'ENISA coopère sur les questions liées à la cybersécurité avec d'autres organes de l'Union, y compris le comité européen de la protection des données, afin d'assurer la cohérence, de créer des synergies et de traiter les questions d'intérêt commun. Cette coopération peut être assurée par l'échange de savoir-faire et de bonnes pratiques; la fourniture de conseils et de lignes directrices sur des questions liées à la cybersécurité; ainsi que par la mise en place de modalités pratiques pour l'exécution de tâches spécifiques, après consultation de la Commission.
17. Le comité et le Contrôleur se félicitent de la coopération et des synergies entre l'ENISA et d'autres entités de l'Union, conformément à leurs missions et mandats respectifs. Dans ce contexte, par souci de clarté juridique, le comité et le Contrôleur recommandent de modifier l'article 68 de la proposition CSA2 en ajoutant une référence explicite au Contrôleur en tant qu'organe de l'Union, avec lequel l'ENISA coopérerait¹¹.

4 COOPÉRATION OPÉRATIONNELLE, CONNAISSANCE COMMUNE DE LA SITUATION EN MATIÈRE DE CYBERSÉCURITÉ ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

18. En vertu des articles 10 et 11 de la proposition CSA2, qui constituerait un développement supplémentaire de l'actuel article 7 du règlement sur la cybersécurité, l'ENISA élargirait son rôle de pôle central pour la coopération opérationnelle, y compris le traitement d'importants volumes de renseignements sur les menaces¹². En conséquence, on pourrait en déduire que les informations traitées par l'ENISA dans le cadre de son rôle peuvent inclure des données à caractère personnel, telles que des adresses IP, des identifiants d'utilisateur, des journaux d'utilisateurs, des échanges financiers ou des détails de comptes compromis.

¹⁰ En prévoyant la participation de l'ENISA à la demande des autorités de contrôle, un processus consultatif structuré est maintenu, dans le cadre duquel l'ENISA fournit une expertise technique tandis que les autorités de contrôle conservent le contrôle total des décisions relatives à la protection des données. Cela garantit également que toute intervention de l'ENISA soit coordonnée, le comité ou le Contrôleur assumant la direction des opérations et déterminant la ligne de conduite appropriée. Ce respect des rôles établis favorise la cohérence, empêche la fragmentation réglementaire et renforce la responsabilité des organismes de protection des données dans leur rôle de surveillance.

¹¹ Le comité et le Contrôleur estiment que l'article 7, paragraphe 2, de l'actuel règlement sur la cybersécurité, qui oblige l'ENISA à coopérer au niveau opérationnel et à établir des synergies avec les institutions, organes et organismes de l'Union, notamment avec les autorités de contrôle chargées de la protection de la vie privée et des données à caractère personnel, en vue de traiter des questions d'intérêt commun, s'étend déjà au Contrôleur.

¹² Voir COM(2026) 11 final, fiche financière et numérique législative, p. 19: «Les nouveaux éléments/tâches figurant dans la proposition apporteront une valeur ajoutée aux parties prenantes européennes, qui profiteront du rôle joué par l'ENISA en tant que pôle d'information contribuant au partage d'informations et fournissant des notifications d'alerte à leurs membres», et p. 95: «Ces dernières années, l'ENISA est devenue un pôle d'information, détenant des informations provenant de différentes sources. En ce sens, bon nombre des tâches de l'ENISA sont associées à la réutilisation et au recyclage des informations aux fins de diverses analyses».

19. À la suite des éclaircissements fournis par la Commission européenne¹³, le comité et le Contrôleur comprennent qu'aucun traitement à grande échelle de données à caractère personnel par l'ENISA n'est destiné à être mandaté et autorisé par le CSA2¹⁴.

Tout en prenant note du fait que l'ENISA collecterait et traiterait principalement des données agrégées à caractère non personnel, le comité et le Contrôleur rappellent néanmoins que si les futures tâches de l'ENISA en tant que pôle d'information nécessitaient un traitement de données à caractère personnel d'une ampleur considérable, cela devrait être explicitement énoncé dans les dispositions de l'acte de base régissant les missions respectives, y compris les éléments essentiels de tout traitement à grande échelle et les garanties appropriées. À l'inverse, si l'objectif est de permettre à l'ENISA de collecter et de traiter ultérieurement principalement des données agrégées à caractère non personnel, cela devrait également être précisé, au moins au moyen d'un considérant.

20. Le comité et le Contrôleur notent que l'ENISA continuerait à traiter des données à caractère personnel à des fins administratives¹⁵. L'article 66, paragraphe 1, de la proposition CSA2, à l'instar de l'actuel règlement CSA¹⁶, contient une référence générale à la législation applicable en matière de protection des données, à savoir le RPDUE, sans prévoir d'autres règles spécifiques.
21. Dans le même ordre d'idées, l'article 66, paragraphe 2, de la proposition CSA2 reproduit l'actuel article 41, paragraphe 2, de l'actuel règlement sur la cybersécurité, qui prévoit la possibilité pour le conseil d'administration de l'ENISA d'adopter des «mesures supplémentaires nécessaires pour l'application du règlement (UE) 2018/1725» par l'Agence¹⁷, sans obligation pour le conseil d'administration de prendre des mesures spécifiques. La disposition de l'article 66, paragraphe 2, de la proposition CSA2 ne précise ni le champ d'application ni la nature de ces mesures supplémentaires de protection des données, ni la procédure applicable pour leur adoption. Elle ne clarifie pas non plus le rôle du Contrôleur dans le processus¹⁸.
22. Le comité et le Contrôleur comprennent que si le conseil d'administration de l'ENISA procède à l'application de l'article 66, paragraphe 2, de la proposition CSA2, sa ou ses décisions devraient fournir des détails supplémentaires sur la manière dont l'ENISA procède au traitement des données à caractère personnel.

¹³ Comme indiqué lors d'une réunion ad hoc du sous-groupe d'experts en technologie du comité le 27 février 2026.

¹⁴ La Commission a précisé que l'ENISA n'avait pas pour mandat de procéder à une analyse opérationnelle des incidents et qu'elle n'avait pas accès aux données provenant des incidents eux-mêmes. Au lieu de cela, le traitement des données sera agrégé. Les alertes des centres de réponse aux incidents de sécurité informatique (CSIRT) nationaux ne comprendront généralement pas de données opérationnelles à caractère personnel, mais plutôt des données administratives telles que les coordonnées. Dans le même ordre d'idées, les entreprises qui s'abonnent pour recevoir des alertes précoces pourraient également fournir leurs coordonnées. Selon la Commission européenne, dans le cas rare où les informations agrégées sur les menaces ou les incidents fournies à l'ENISA contiennent des adresses IP, l'ENISA n'aurait aucun besoin opérationnel et, par conséquent, aucune possibilité juridique et factuelle d'enquêter sur l'abonné derrière l'adresse IP. La Commission européenne précise en outre que le service d'assistance prévu à l'article 13 est de nature consultative et fournit, par exemple, des informations sur l'autorité compétente de l'État membre à contacter.

¹⁵ Par exemple, dans le cadre du processus d'examen des demandes d'agrément en tant que fournisseur d'attestation au titre du programme d'attestation individuelle européenne des compétences en matière de cybersécurité (article 22), au cours de la procédure de recours contre les décisions prises (articles 36 et suivants), lors du traitement des plaintes déposées par des personnes physiques ou morales en ce qui concerne la certification ou les déclarations de conformité de l'Union [article 88, paragraphe 6, point h)] ou en ce qui concerne les certifications de cybersécurité (article 96).

¹⁶ Article 41, paragraphe 1, du règlement (UE) 2019/881.

¹⁷ Le 21 novembre 2019, le conseil d'administration de l'ENISA a adopté la décision relative aux règles internes concernant la limitation de certains droits des personnes concernées en matière de traitement des données à caractère personnel dans le cadre du fonctionnement de l'ENISA, conformément à l'article 25 du RPDUE.

¹⁸ Par exemple, l'article 18 *bis*, paragraphe 5, du règlement (UE) 2016/794 (règlement Europol) prévoit que le conseil d'administration d'Europol, sur proposition du directeur exécutif et **après consultation du Contrôleur**, précise les conditions relatives à la fourniture et au traitement des données à caractère personnel [...] (caractères gras ajoutés).

23. Le comité et le Contrôleur rappellent qu'en principe, seuls les détails très techniques (pratiques) liés au traitement des données à caractère personnel devraient être laissés à l'appréciation du conseil d'administration d'une agence décentralisée, dans le cadre de l'autonomie administrative de l'organe de l'Union concerné, en l'occurrence. En effet, l'autorisation des ingérences dans les droits fondamentaux devrait être une question mieux réservée au législateur et, tout au plus, à la Commission au moyen d'actes d'exécution ou d'actes délégués¹⁹. Par conséquent, il convient donc de préciser explicitement, dans le dispositif du règlement, ce que signifie exactement la deuxième phrase du projet d'article 66, paragraphe 2, par «mesures supplémentaires nécessaires pour l'application du règlement (UE) 2018/1725 par l'ENISA».
24. S'il est néanmoins jugé nécessaire que le conseil d'administration prenne des mesures allant au-delà des modalités techniques (pratiques) du traitement déjà prévues dans la législation ou des actes délégués ou d'exécution, en plus de définir plus clairement leur champ d'application, les mesures que le conseil d'administration doit adopter devraient être claires et précises, et leur application devrait être prévisible pour les personnes concernées. Ces règles font notamment l'objet d'une publicité appropriée. En outre, elles devraient prévoir les garanties nécessaires pour assurer le respect des principes et garanties clés en matière de protection des données, tels que la limitation de la finalité, la limitation de la conservation et la protection des données dès la conception et par défaut. En outre, à titre de garantie supplémentaire importante dans de tels cas, le comité et le Contrôleur recommandent que l'article 66 de la proposition CSA2 prévoie une consultation préalable du Contrôleur avant l'adoption de ces règles²⁰.

5 POINT D'ENTRÉE UNIQUE POUR LA NOTIFICATION DES INCIDENTS (ARTICLE 15 DE LA PROPOSITION CSA2)

25. Conformément à l'article 15 de la proposition CSA2, l'ENISA doit établir, fournir, exploiter, gérer et mettre à jour en tant que de besoin, entre autres, la plateforme unique de signalement établie en vertu de l'article 16, paragraphe 1, du règlement (UE) 2024/2847 et le point d'entrée unique pour le signalement des incidents établi en vertu de l'article 23 *bis* de la directive (UE) 2022/2555. Ces outils visent à simplifier les différentes obligations de déclaration liées à la cybersécurité²¹.

¹⁹ Voir le document intitulé «Guidance for co-legislators on key elements of legislative proposals» (Orientations à l'intention des colégislateurs sur les éléments clés des propositions législatives) du Contrôleur, disponibles à l'adresse https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, point 76.

²⁰ À l'instar de ce qui est prévu à l'article 18 *bis*, paragraphe 5, du règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (règlement Europol) (JO L 135 du 24.5.2016, p. 53).

²¹ Voir article 16, paragraphe 1, du règlement (UE) 2024/2847 et COM(2025) 837 final, p. 8.

26. Comme déjà indiqué dans leur avis conjoint sur la proposition «omnibus numérique»²², le comité et le Contrôleur soutiennent fermement l'objectif de la mise en place d'un point d'entrée unique pour la notification des violations de données à caractère personnel, car cela réduirait la charge administrative pour les organisations sans affecter le niveau de protection des personnes concernées. Dans sa déclaration d'Helsinki²³, le comité a déjà souligné son soutien à une éventuelle solution européenne de notification transréglementaire, car cela contribuerait à faciliter le respect du RGPD. Le comité et le Contrôleur rappellent également qu'il importe de garantir la sécurité des notifications soumises au point d'entrée unique et transmises par son intermédiaire, étant donné que les notifications de violation de données contiennent souvent des informations sensibles²⁴.

6 CADRE EUROPÉEN DES COMPÉTENCES EN MATIÈRE DE CYBERSÉCURITÉ (ECSF) (ARTICLE 19 DE LA PROPOSITION CSA2)

27. L'article 19 de la proposition CSA2 exigerait que l'ENISA élabore et mette à la disposition du public un cadre européen des compétences en matière de cybersécurité (ci-après l'«ECSF»). L'ECSF contribuerait à faire en sorte que les professionnels de la cybersécurité, les employeurs, les prestataires de formation et les autorités publiques dans l'ensemble des États membres partagent une vision commune des compétences requises pour les différents postes dans le domaine de la cybersécurité. Il favoriserait des profils d'emploi clairs, des exigences transparentes en matière de qualifications et une meilleure adéquation entre l'enseignement et les besoins du marché du travail. L'ENISA utiliserait l'ECSF comme base pour dispenser des formations, en particulier pour soutenir la mise en œuvre de la législation de l'Union en matière de cybersécurité, la coopération opérationnelle entre les États membres et les activités de sensibilisation. Cela signifie que l'ECSF sert de base à des programmes structurés de formation à la cybersécurité, en particulier pour les autorités publiques et les entités couvertes par la législation de l'Union en matière de cybersécurité.
28. Le comité et le Contrôleur se félicitent de l'objectif consistant à renforcer la main-d'œuvre de l'Union dans le domaine de la cybersécurité et soulignent qu'il est important, pour le bon fonctionnement du marché unique numérique, de rendre les compétences plus transférables et reconnaissables par-delà les frontières.

²² [Avis conjoint du comité européen de la protection des données et du Contrôleur européen de la protection des données \[2/2026\] concernant la proposition de règlement relative à la simplification du cadre législatif numérique \(train de mesures omnibus sur le numérique\), adopté le 10 février 2026.](#)

²³ comité européen de la protection des données, [Déclaration d'Helsinki sur le renforcement de la clarté, du soutien et de l'engagement](#), Une approche de l'innovation et de la compétitivité fondée sur les droits fondamentaux, adoptée le 2 juillet 2025.

²⁴ Voir le chapitre 8.3 de l'[avis conjoint du comité européen de la protection des données et du Contrôleur européen de la protection des données \[2/2026\] concernant la proposition de règlement relative à la simplification du cadre législatif numérique \(train de mesures omnibus sur le numérique\), adopté le 10 février 2026.](#)

29. Dans le même temps, ils notent que les profils définis à l'article 19, paragraphe 2, de la proposition CSA2 sont actuellement limités aux professionnels de la cybersécurité. La proposition ne comprend pas de profil de compétences nécessaires pour les citoyens, les fonctionnaires ou les membres non spécialisés de la main-d'œuvre. Comme le reconnaît le considérant 21 de la proposition CSA2, l'habileté numérique est essentielle pour donner aux citoyens résilients les moyens d'agir, mais près de la moitié de la population adulte ne possède pas les compétences numériques de base, bien que plus de 90 % des emplois le requièrent. Par conséquent, l'ECSF devrait inclure un profil «Cybersécurité pour les généralistes», qui couvrirait les compétences minimales que chaque résident de l'Union en âge de travailler devrait posséder pour interagir en toute sécurité au sein du marché unique numérique, en se protégeant non seulement lui-même, mais aussi son organisation et les autres, notamment contre le hameçonnage assisté par l'intelligence artificielle, les hypertrucages, l'usurpation d'identité et les attaques d'ingénierie sociale. Ce profil pourrait être utilisé par des organisations publiques ou privées pour former leur personnel afin de réduire au minimum les risques liés au facteur humain, réduisant ainsi le risque global de violation des données.
30. Le comité et le Contrôleur notent que le considérant 45 de la proposition distingue explicitement l'ECSF du cadre européen des compétences numériques (DigComp 3.0), en précisant que ce dernier est destiné à la vie quotidienne, à la participation à la société, au travail et à l'apprentissage, et peut être utilisé tant par les adultes que par les enfants²⁵, tandis que l'ECSF est destiné à un public spécialisé, offrant un cadre simple recensant les rôles en matière de cybersécurité et les tâches, connaissances et compétences associées nécessaires à leur exécution.
31. Le comité et le Contrôleur soutiennent toutes les initiatives mentionnées, qu'elles soient mises en œuvre par l'ENISA ou, dans le cas de DigComp, par le Centre commun de recherche (JRC) de la Commission européenne, car elles permettraient, pour autant qu'elles soient largement adoptées, de réduire le risque de violation des données. Par conséquent, ils encouragent toutes les parties concernées à étudier les moyens d'accroître l'incidence des cadres.

²⁵ Le comité et le Contrôleur rappellent en outre qu'entre 2022 et 2024, la Commission européenne a étudié l'élaboration d'un certificat européen de compétences numériques, fondé sur DigComp. Le certificat aiderait les personnes à faire reconnaître rapidement et facilement leurs compétences numériques par les employeurs, les prestataires de formation, etc. Cette initiative visait à offrir un label de qualité pour la certification des compétences numériques dans toute l'Europe. À la suite d'une étude de faisabilité (voir CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., Hüsing, T., CUARTAS-ACOSTA, A. et TROIA, S., European Digital Skills Certificate (EDSC) Feasibility Study (Étude de faisabilité du certificat européen de compétences numériques), Office des publications de l'Union européenne, Luxembourg, 2024, doi: 10.2760/958195, JRC138344, <https://publications.jrc.ec.europa.eu/repository/handle/JRC138344>) et d'un projet pilote mené avec plusieurs pays de l'Union, la Commission européenne a conclu qu'un tel label de qualité n'apporterait pas suffisamment de valeur ajoutée aux citoyens européens. Toutefois, DigComp, publié pour la première fois en 2013, existe toujours (COSGROVE, J. et CACHIA, R., DigComp 3.0: European Digital Competence Framework - Fifth Edition (Cadre européen des compétences numériques – Cinquième édition), Office des publications de l'Union européenne, Luxembourg, 2025, <https://data.europa.eu/doi/10.2760/0001149>, JRC144121). Il décrit ce qui est nécessaire pour être compétent sur le plan numérique dans la société d'aujourd'hui et soutient le développement des compétences numériques parmi les individus de tous âges. Il couvre un large éventail de niveaux de compétences, des plus élémentaires aux plus avancés. Plusieurs compétences de DigComp font explicitement référence à la cybersécurité, telles que 4.1 Protéger les appareils numériques, 4.2 Protéger les données personnelles et la vie privée et même 4.4 Protéger l'environnement (prévention des fuites de données provenant d'équipements mis au rebut). D'autres domaines concernent également des compétences pertinentes: ainsi, les compétences du domaine 1 sont essentielles pour se prémunir contre l'ingénierie sociale, celles du domaine 2 permettent de réduire les risques liés aux menaces internes et d'éviter la divulgation accidentelle d'informations, tandis que celles du domaine 5 améliorent la rapidité de détection des incidents.

32. Dans le même temps, le comité et le Contrôleur considèrent que DigComp ne remplace pas un schéma de cybersécurité spécifique pour les généralistes²⁶ et recommandent aux colégislateurs de modifier l'article 19, paragraphe 2, de la proposition CSA2 afin que l'ECSF ne se limite pas exclusivement aux «professionnels de la cybersécurité», mais comprenne également des profils pour la main-d'œuvre en général ou les citoyens. Cette modification devrait s'accompagner d'un amendement correspondant au considérant 45.
33. En outre, le comité et le Contrôleur estiment qu'il est nécessaire que les profils professionnels de l'ECSF intègrent un module sur la nécessité de garantir la conformité des mesures de cybersécurité avec la législation de l'Union en matière de protection des données, en particulier en ce qui concerne la mise en œuvre pratique du principe de protection des données dès la conception et par défaut (article 25 du RGPD), et invitent le colégislateur à ajouter un considérant à cet objectif.

7 CADRE EUROPÉEN DE CERTIFICATION DE CYBERSÉCURITÉ (TITRE III)

34. L'article 71 et l'article 80, paragraphe 1, point w), de la proposition CSA2 régissent le champ d'application de la certification de cybersécurité. L'article 80, paragraphe 1, point w), ajoute l'élément suivant en tant qu'objectif de sécurité pour les schémas européens de certification de cybersécurité: «veiller à ce que l'entité soit en mesure d'assurer la sécurité du traitement des données à caractère personnel».
35. Le comité et le Contrôleur notent que le libellé de l'article 80, paragraphe 1, point w), de la proposition CSA2 est très proche des exigences du RGPD en matière de sécurité du traitement²⁷. En ce sens, le champ d'application du nouveau système de certification pourrait être interprété comme incluant des exigences au titre du RGPD. Toutefois, le champ d'application juridique et opérationnel n'est pas tout à fait clair, étant donné que la disposition ne renvoie pas aux dispositions du RGPD [par exemple, l'article 5, paragraphe 1, point f), l'article 32 et l'article 25 du RGPD] et qu'elle figure dans une liste d'«objectifs de sécurité» (article 80, paragraphe 1, première phrase).
36. Le comité et le Contrôleur rappellent que la sécurité au titre du RGPD est liée aux risques pour les libertés et droits fondamentaux des personnes. Si la définition juridique de la cybersécurité dans le droit de l'Union inclut largement la protection des utilisateurs et d'autres personnes²⁸, le champ d'application des mesures de cybersécurité englobe généralement tous les types de risques pour l'organisation concernée. Il est néanmoins possible d'établir des synergies afin que l'évaluation des risques puisse intégrer la protection des droits et libertés des personnes.

²⁶ Dans DigComp, le contenu relatif à la sécurité est réparti entre 21 compétences; il ne comporte pas de modèles de menace explicites, il ne prend pas en considération les risques de sécurité organisationnels et il ne correspond pas directement aux obligations de conformité. Alors que l'ECSF, dans sa forme actuelle, s'appliquerait aux compétences des professionnels de la cybersécurité, il n'existe pas de cadre structuré au niveau de l'Union pour les employés qui ne travaillent pas dans le domaine de la cybersécurité. Le comité et le Contrôleur rappellent que la plupart des violations de données trouvent leur origine dans l'hameçonnage, l'ingénierie sociale, l'utilisation abusive d'identifiants, les erreurs de configuration et le recours à l'«informatique fantôme». Il s'agit de comportements généralistes. Un cadre généraliste en matière de cybersécurité pourrait mettre en évidence les risques, formuler des attentes adaptées aux rôles (par exemple en ce qui concerne les ressources humaines et les finances) et favoriser l'obtention de résultats mesurables.

²⁷ Voir l'article 5, paragraphe 1, point f), et l'article 32 du RGPD.

²⁸ Voir l'article 2, paragraphe 1, de la proposition CSA2, qui est une disposition ancienne et dont le libellé est le suivant: «cybersécurité»: les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces.

37. Le comité et le Contrôleur rappellent en outre que le RGPD dispose de son propre mécanisme de certification (articles 42 à 43 du RGPD) et considèrent que la certification de cybersécurité est distincte de la certification en matière de protection des données conformément à l'article 42 du RGPD.
38. Cela étant dit, le comité et le Contrôleur estiment qu'il peut y avoir des synergies entre la certification en matière de cybersécurité et la certification en matière de protection des données. Par exemple, la certification CSA2 pourrait être utilisée comme preuve à l'appui pour démontrer que certaines exigences d'une certification du RGPD sont remplies, en ce qui concerne la cybersécurité. Toutefois, le comité et le Contrôleur notent que l'article 80, paragraphe 1, point w), de la proposition CSA2 n'établit pas clairement le lien avec la certification au titre des articles 42 et 43, du RGPD. Dans un souci de sécurité juridique, le comité et le Contrôleur recommandent de clarifier davantage le champ d'application de l'article 80, paragraphe 1, point w), de la proposition CSA2 et le lien avec la certification du RGPD. En outre, le comité et le Contrôleur recommandent d'exiger de l'ENISA qu'elle consulte le comité avant d'adopter un système de certification au titre de l'article 80, paragraphe 1, point w), de la proposition CSA2, afin de garantir la cohérence.
39. Le comité et le Contrôleur soulignent l'importance de tenir compte non seulement de l'efficacité des mesures de cybersécurité, mais aussi de leur nécessité et de leur proportionnalité. Certains contrôles de cybersécurité créent des risques spécifiques en matière de protection des données. Cela peut être le cas de la surveillance et de la journalisation, de l'inspection approfondie des paquets ou de l'analyse du comportement des utilisateurs. Un système de certification bien conçu pour la sécurité du traitement pourrait inclure des contrôles visant à garantir que les mesures de sécurité peuvent être mises en œuvre dans le respect des règles en matière de protection des données (par exemple, certains aspects devraient être configurables; cela pourrait être le cas, par exemple, de la granularité des données enregistrées à des fins de sécurité, car cela peut permettre ou faciliter le respect par le responsable du traitement des principes de sécurité et de minimisation des données énoncés dans le RGPD; dans le même ordre d'idées, les durées de conservation devraient être configurables afin que le responsable du traitement puisse décider, dans le cadre du traitement qu'il met en œuvre, de la durée pendant laquelle les données à caractère personnel devraient être conservées avant d'être supprimées ou anonymisées à l'aide de techniques certifiées).
40. Par conséquent, le comité et le Contrôleur recommandent d'expliquer dans un considérant que les systèmes de certification devraient, dans la mesure du possible, être conçus, mis en œuvre et entretenus de manière à tenir compte des contrôles de sécurité susceptibles de contribuer à démontrer le respect des exigences du RGPD, lorsque les systèmes s'appliquent aux produits TIC, aux services TIC, aux processus TIC et aux services de sécurité gérés susceptibles d'être utilisés dans des opérations de traitement de données. Il convient également de noter que certains contrôles peuvent faciliter la protection de la vie privée et des données dès la conception et par défaut.

8 CADRE DE CONFIANCE POUR LA CHAÎNE D'APPROVISIONNEMENT DES TIC (TITRE IV)

41. La proposition CSA2 ajoute des mesures pour la sécurité des chaînes d'approvisionnement des TIC, en s'attaquant notamment aux risques non techniques, tels que les facteurs géopolitiques, juridiques, liés à la propriété, à la dépendance et aux ingérences stratégiques qui affectent les chaînes d'approvisionnement des TIC dans les secteurs hautement critiques et d'autres secteurs critiques. Si ces mesures de sécurité de la chaîne d'approvisionnement visent principalement à faire face à des risques qui ne sont pas directement liés à la protection des données, elles peuvent également avoir une incidence bénéfique sur la protection des droits fondamentaux en limitant l'ingérence étrangère dans les données des personnes concernées de l'Union au moyen d'activités telles que l'espionnage et la surveillance.
42. Le comité et le Contrôleur se félicitent de la mesure proposée visant à garantir un cadre de confiance pour la chaîne d'approvisionnement des TIC et à faire face aux risques non techniques dans les secteurs hautement critiques.

9 ENTITÉS ESSENTIELLES SUPPLÉMENTAIRES AU TITRE DE LA PROPOSITION DE MODIFICATION DE LA DIRECTIVE SRI 2

43. La proposition modifiant la directive SRI 2 inclurait les portefeuilles européens d'identité numérique et les fournisseurs de portefeuilles européens d'identité numérique pour les entreprises, en tant qu'«entités essentielles», quelle que soit leur taille. Les entités classées comme «essentielles» sont soumises à l'ensemble des obligations en matière de gestion des risques de cybersécurité prévues par la directive SRI 2 et doivent mettre en œuvre les mesures de sécurité requises en vertu de l'article 21 de la directive SRI 2, notamment l'analyse des risques et les politiques de sécurité, la gestion des incidents, la continuité des activités et la gestion des crises, la sécurité de la chaîne d'approvisionnement, la gestion des vulnérabilités, les politiques en matière de cryptographie et de chiffrement, ainsi que le contrôle d'accès et la gestion des actifs.
44. Le comité et le Contrôleur se félicitent de la désignation des portefeuilles européens d'identité numérique et des fournisseurs de portefeuilles européens d'identité numérique pour les entreprises en tant qu'«entités essentielles». Le comité et le Contrôleur considèrent que les portefeuilles d'identité numérique sont une composante essentielle de l'infrastructure numérique de l'Union, de sorte que les incidents qui les concernent pourraient avoir une large incidence transfrontière. Ils sous-tendent l'identification, l'authentification et les attestations électroniques sécurisées. Pour l'économie numérique, les portefeuilles d'entreprises sont tout aussi essentiels que les portefeuilles européens d'identité numérique. Par conséquent, les deux types de fournisseurs de portefeuilles sont traités de la même manière que les prestataires de services de confiance, qui ont déjà été désignés comme des «entités essentielles» au titre de la directive SRI 2, et que d'autres opérateurs d'infrastructures hautement critiques.

10 COLLECTE DE DONNÉES SUR LES ATTAQUES PAR RANÇONGICIEL

45. Conformément à l'article 1^{er}, paragraphe 8, de la proposition de modification de la directive SRI 2, qui propose d'ajouter de nouveaux paragraphes 12 et 13 à l'article 23 de la directive SRI 2, en cas d'attaque par rançongiciel, les entités concernées peuvent être invitées à communiquer certaines informations concernant les incidents liés aux rançongiciels aux CSIRT, y compris si une entité a payé une rançon et, dans l'affirmative, quel montant et à qui (crypto-actifs/prestataires de services) et l'identité de la personne agissant en tant que point de contact.
46. En vertu de l'article 23, paragraphe 11, de la directive SRI 2, la Commission est habilitée à adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure des obligations en matière de rapports. Le champ d'application de cet acte d'exécution serait étendu pour couvrir également les nouvelles obligations de déclaration en cas d'attaques par rançongiciel.
47. Le comité et le Contrôleur soutiennent pleinement l'objectif important consistant à prévenir de futures attaques par rançongiciel et à perturber et démanteler les organisations criminelles qui en sont à l'origine. Le comité et le Contrôleur notent que les informations à partager concernant les attaques par rançongiciel pourraient être de nature potentiellement sensible, comme l'explique plus en détail la Commission au considérant 10 de la proposition de modifications de la directive SRI 2. En outre, ces rapports peuvent impliquer le traitement de données à caractère personnel. Le comité et le Contrôleur se félicitent de l'approche par étapes choisie aux paragraphes 12 et 13, selon laquelle les informations plus sensibles visées au paragraphe 13 ne seront communiquées que sur demande.
48. Dans le même temps, compte tenu du caractère sensible des données communiquées et conformément aux principes de nécessité et de proportionnalité, dans le cas où le signalement d'attaques par rançongiciel impliquerait le traitement de données à caractère personnel, le comité et le Contrôleur recommandent de préciser, dans l'acte d'exécution conformément à l'article 23, paragraphe 11, de la directive SRI 2, les garanties applicables en matière de protection des données. À cet égard, ils rappellent également l'obligation pour la Commission, en vertu de l'article 42, paragraphe 1, du RPDUE, de consulter le Contrôleur sur les projets d'actes d'exécution et d'actes délégués lorsqu'il existe une incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel.