INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

RESULTAT DE LA CONSULTATION PUBLIQUE NATIONALE (CP/N26/1) DU 6 JUILLET 2026 AU 31 AOUT 2026

CONCERNANT LE PROJET DE REGLEMENT PORTANT SUR LA NOTIFICATION DES MESURES DE SÉCURITÉ PRISES PAR LES ENTITÉS ESSENTIELLES

LUXEMBOURG, LE 2 NOVEMBRE 2026

SECTEUR NISS

---

1. Introduction et contexte

Le présent document constitue la prise de position de l'Institut luxembourgeois de régulation (ci-après « Institut » ou « ILR ») suite aux avis et commentaires reçus lors de la consultation publique relative au projet de règlement portant sur la notification des mesures de sécurité prises par les entités essentielles dans le cadre de la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité (ci-après « loi NIS2 »). Le processus de la consultation publique nationale est de ce fait clôturé.

L'Institut remercie tous les contributeurs pour leurs commentaires et leurs suggestions. Dans la présente prise de position, l'Institut se concentrera en priorité sur les contributions les plus ciblées sur les enjeux majeurs.

Dans un souci de protection des intérêts des différentes parties en cause et de leur anonymat, les contributions sont traitées de manière confidentielle et ne sont pas accessibles au public.

2. Contributions rendues anonymes

Contributions sur la forme

L'Institut a reçu quelques contributions concernant la forme du règlement, notamment la numérotation des articles.

Il a été porté à l'attention de l'Institut que l'article 4 du projet de règlement comporte 2 paragraphes portant le numéro « (2) ». Aux fins de redressement, l'Institut modifiera le numéro du dernier paragraphe comme suit : « **(3)** ».

Ensuite, une entité a soulevé une différence de dénomination à l'article 4 du projet de règlement, notamment l'utilisation alternative des termes « *plan pluriannuel d'actions* » et « *plan d'action pluriannuel* ». Dans un souci de cohérence, le terme unique utilisé sera celui de « ***plan d'action pluriannuel*** ». En ce sens, l'Institut veillera à revérifier l'intégralité du projet de règlement et à appliquer le même terme partout où besoin sera.

Contributions sur le fond

L'Institut a reçu diverses contributions concernant le contenu du règlement, notamment les informations requises, leurs contenu et leur procédure de transmission.

a. Clarification des procédures de transmission de livrables et de documents/informations

Différentes entités ont souhaité avoir plus de clarification quant au format de soumission d'informations ou de documents.

En principe, tous les échanges d'informations ou de documents devront être fait par un moyen sécurisé, soit directement déterminé dans les règlements ILR (tel que p. ex. via la plateforme SERIMA), soit déterminé et accepté par l'Institut individuellement. Ceci est dûment repris à l'Article 7 du règlement sous analyse.

L'évolution des moyens sécurisés de transmission des documents/informations sera communiquée aux entités dans les meilleurs délais.

Toute modification ou ajout au niveau des livrables sera communiqué aux entités dans les meilleurs délais. Les livrables seront assortis d'un numéro de version et de la date de modification.

Quant aux délais de remise des informations, une distinction est à faire entre les documents exigés annuellement et les documents demandés ponctuellement ou en supplément :

- Pour les livrables annuels : la date est fixée au 15 mars de chaque année (date prévue dans le règlement sous analyse).
- Pour toute autre demande d'information : les demandes d'information sont assorties d'un délai raisonnable permettant à l'entité de réunir toutes les informations requises. Le délai prévu dans les demandes d'information est proportionné à la demande formulée et à sa complexité, et ainsi déterminé au cas par cas.

b. <u>Précision des obligations légales relatives aux livrables annuels</u>

L'Institut souhaite attirer l'attention des entités sur le fait que la remise des livrables élaborés par l'Institut et disponibles sur son site internet, ne se substitue pas aux obligations *internes* en matière de cybersécurité. Le caractère limité des livrables ne substitue pas une gestion des risques adéquate et proportionnée en interne. Toute entité devra réaliser des analyses de risques internes pour son propre compte, bien que celles-ci ne devront plus être remises à l'Institut annuellement.

Quant à tout autre outil (p.ex. MONARC) utilisé par les entités pour leur propre gestion des risques interne, ceux-ci peuvent toujours être utilisés. Néanmoins, aucun document ou rapport (p.ex. analyse de risque MONARC) ne saurait substituer un quelconque livrable requis dans le cadre du présent projet de règlement.

Ensuite, l'Institut a reçu diverses contributions concernant l'équivalence des standards et normes tels que les certificats ISO. L'Institut souhaite souligner qu'un certificat ISO peut être référencé comme preuve/évidence pour une ou plusieurs mesures de sécurité. Néanmoins, une certification ISO ne se substitue pas aux livrables requis en vertu des règlements ILR. De même, une certification ISO ne permet pas de présumer la conformité avec les exigences et les obligations de la loi NIS2.

Le même raisonnement s'applique pour tout type de certification, de plan d'action ou d'évaluation de risques, tels que par exemple les plans de résilience ou le Plan de préservation numérique en matière d'archivage.

Eu égard à une contribution concernant le contenu des livrables, l'Institut souhaite soulever le fait que les livrables sont majoritairement basés sur des documents élaborés au niveau européen. Il en est le cas notamment pour le document intitulé « Description des mesures en place », qui est principalement basé sur le document de référence élaboré au niveau du groupe de coopération européen (« NIS CG ») établi en vertu de l'article 14 de la directive SRI 2[1].

Diverses contributions ont soulevé le fait que le livrable « liste des dépendances » ne soit pas limité selon le niveau de criticité de la dépendance. L'objectif de la loi NIS2 étant d'améliorer le niveau de cybersécurité des entités de manière efficace et sur le long terme, il est important pour les entités d'avoir une vue globale sur l'étendue de leurs dépendances. La priorité peut être donnée aux dépendances les plus critiques, mais toute autre dépendance moins critique devra néanmoins faire l'objet d'un recensement. Le niveau de criticité ne peut être établi qu'après avoir recensé toutes les dépendances existantes, ce qui réduit aussi le risque d'oubli de l'une ou l'autre dépendance. En ce sens, le projet de règlement sous analyse ne peut pas prévoir de limitation.

[1] 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 o 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

c. <u>Contributions diverses</u>

Une entité a soulevé une question relative à la protection des données et à la légitimité sous le règlement général sur la protection des données[2] pour l'information requise sous l'article 4 (2), point e) du projet de règlement, notamment la désignation nominative d'un « responsable » pour l'exécution de l'action prévue dans le plan d'action pluriannuel.
Considérant que l'élément pertinent dans le cadre du plan d'action pluriannuel est d'assurer le suivi et l'exécution de ladite action, il conviendrait de désigner « un rôle » (stable) plutôt qu'une « personne » (dynamique). En ce sens, l'Institut modifiera l'article 4 (2), point e) du projet de règlement comme suit :
« *e) le **rôle** responsable pour l'exécution de l'action en question ;* »

Suite à une contribution concernant la mise en relation de la « description des mesures de sécurité » et du « plan d'action pluriannuel », l'Institut souhaite préciser qu'il revient à chaque entité en fonction de sa maturité et de ses priorités de déterminer quelles sont les actions à entreprendre afin d'améliorer ses mesures de sécurité. Donc, un report automatique d'une mesure de sécurité non-implémentée référencée dans la « description des mesures de sécurité » vers le « plan d'action pluriannuel » ne correspondrait pas à la réalité.

Ensuite, diverses contributions ont soulevé l'obligation de sécurisation de la chaîne d'approvisionnement, reprise aussi à l'article 2 paragraphe 1er, point f) du projet de règlement sous analyse. En effet, la loi NIS2 institue le principe de sécurité de la chaîne d'approvisionnement comme responsabilité imposée à l'entité tombant dans son champ d'application. Cette responsabilité repose intégralement sur l'entité NIS2 en tant que fournisseur de ses propres services : il est de sa responsabilité de garantir un niveau de cybersécurité tout au long de sa chaîne d'approvisionnement. Pour ce faire, l'entité peut par exemple prévoir des clauses de sécurité dans ses contrats de sous-traitance ou avec ses fournisseurs, de même que demander à ses fournisseurs de fournir des informations sur leurs mesures de sécurité en place. L'Institut souhaite attirer l'attention des entités sur le fait que le service fourni reste la responsabilité de l'entité NIS2, et ceci nonobstant tout fournisseur externe de la chaîne d'approvisionnement. Bien qu'un service ou une partie de celui-ci puisse être sous-traité ou fourni par un prestataire externe, **la responsabilité incombant à l'entité NIS2 n'est jamais transférée.**

Une entité a soulevé le manque de proportionnalité quant à la fréquence de la notification des mesures, plus particulièrement la notification « à chaque fois qu'un changement de la situation rend de nouvelles mesures nécessaires pour assurer un niveau de sécurité adapté ou approprié aux risques existant ». Au regard du principe de proportionnalité et de l'approche fondée sur les risques, l'entité a suggéré la formulation suivante : *« à chaque **changement significatif du niveau de risque, ou de l'identification d'un***

[2] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après « RGPD »)

nouveau risque majeur, ou d'une mise en œuvre de mesures de sécurité particulièrement importantes. »

Pour rappel, l'Institut souhaite rappeler qu'aucun livrable n'est à remettre pour l'année 2026. La prochaine échéance applicable à **tous les secteurs** est le 15 mars 2027.

Pour finir, l'Institut souhaite préciser que les cadres légaux **NIS2** et **CER** sont complémentaires. Dans une optique de simplification administrative, les autorités compétentes respectives s'efforcent à réduire la charge administrative pour les entités et à garantir une supervision efficace et coordonnée.