INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

RÉSULTAT DE LA CONSULTATION PUBLIQUE NATIONALE (CP/N21/6) DU 18 NOVEMBRE 2021 AU 18 DECEMBRE 2021

CONCERNANT LE PROJET DE RÈGLEMENT PORTANT DÉFINITION DES MODALITÉS DE NOTIFICATION ET DES CRITÈRES DES INCIDENTS AYANT UN IMPACT SIGNIFICATIF SUR LA CONTINUITÉ DES SERVICES ESSENTIELS DU SECTEUR SANTÉ

LUXEMBOURG, LE 11 AOÛT 2022

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 définition des modalités de notification et des critères des incidents ayant un impact significatif sur la continuité des services essentiels du secteur santé. Le processus de la consultation publique nationale est de ce fait clôturé.

L'Institut tient compte des commentaires relatifs à l'article 1er (2) et l'article 2 (1) et (2) du projet de règlement émis dans le cadre de la contribution publique susmentionnée.

Contributions rendues anonymes

Quant à l'article 1er (2) du projet de règlement un opérateur souhaite intégrer un lien entre le terme « *incident* » et l'origine de l'incident se trouvant dans « *les domaines des systèmes d'information et biomédicaux institutionnels* ».

L'Institut tient à préciser que le terme « incident » a une connexion inhérente avec les réseaux et systèmes d'information étant donné que ce terme provient de la *loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale* (ci-après la « Loi du 28 mai 2019 »), dans le cadre de laquelle un incident est défini comme étant « *tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information* » (article 2, 6° de la Loi du 28 mai 2019).

Par ailleurs, l'Institut est d'avis qu'un système biomédical tombe sous la définition d'un « réseau et système d'information » au sens de l'article 2, 1° de la Loi du 28 mai 2019.

Cependant, dans un souci de précision, l'Institut intègre dans l'article 1er (1) du projet de règlement une référence aux « réseaux et systèmes d'information ». Ledit paragraphe sera le suivant :

> « *(1) Les opérateurs de services essentiels du secteur santé notifient à l'Institut tous les incidents* ***relatifs aux réseaux et systèmes d'information*** *ayant un impact significatif sur la continuité des services essentiels* ».

En outre, quant à l'article 1er (2) du projet de règlement, un opérateur souhaite remplacer le terme « incident » par le terme « incident confirmé ».

L'Institut est d'avis qu'il n'est pas opportun de dévier à cet endroit de la définition légale d'incident en ajoutant une précision comme « confirmé » pouvant conduire à des interprétations divergentes entre les différents opérateurs de services essentiels du secteur santé.

Toujours quant à l'article 1er (2) du projet de règlement, un opérateur souhaite remplacer la référence à « *l'impact significatif sur la continuité des services essentiels* » par une formulation visant le « *non-maintien prolongé de la continuité des soins d'un ou plusieurs services hospitaliers* ».

ILR 17, rue du Fossé • Adresse postale • L-2922 Luxembourg • T +352 28 228 228 • F +352 28 228 229 • info@ilr.lu www.ilr.lu

Étant donné que le présent projet de règlement vise tous les services essentiels du secteur « santé », il n'est pas opportun de limiter le champ d'application de l'article 1er (2) du projet de règlement.

Finalement, un opérateur souhaite simplifier la liste contenue dans l'article 1er (2) (a) 1° du projet de règlement.

L'Institut rejoint l'opérateur dans l'opportunité de cette simplification et modifie le présent point 1er comme suit :

« *1° Pour l'activité hospitalière :*

- *atteinte réversible sur l'état de santé d'au moins 10 personnes ; ou*
- *atteinte irréversible (dont décès) sur l'état de santé d'une personne* ».

En ce qui concerne l'article 1er (2) (b) du projet de règlement, un opérateur souhaite obtenir des clarifications quant à l'interprétation du terme « 50 personnes ».

L'Institut confirme la compréhension de l'opérateur en ce qui concerne le fait que le terme « personne » ait été choisi afin de pouvoir inclure non seulement les patients d'un opérateur, mais aussi notamment ses collaborateurs, agents et visiteurs.

Le nombre « 50 » a été inséré afin de garder un seuil d'un impact significatif similaire aux règlements de l'Institut relatifs à d'autres secteurs essentiels.

Toujours par rapport à l'article 1er (2) (b) du projet de règlement, un opérateur souhaite compléter cet article par une référence à « *un impact potentiel significatif sur leur* [les 50 personnes] *prise en charge* ».

Toutefois, étant donné que le terme « personne » ne couvre non seulement les patients, mais aussi notamment les collaborateurs, agents et visiteurs des opérateurs des services essentiels du secteur « santé », une référence à une « prise en charge » serait trop restrictive.

Suite à une demande de précision d'un opérateur, l'Institut remplace les termes « système informatique » de l'article 1er (2) (b) du projet de règlement par une référence à un « système d'information ou d'un système biomédical ». L'Institut tient à préciser qu'il comprend néanmoins un système biomédical comme tombant sous la définition d'un « réseau et système d'information » au sens de l'article 2, 1° de la Loi du 28 mai 2019.

ILR 17, rue du Fossé • Adresse postale • L-2922 Luxembourg • T +352 28 228 228 • F +352 28 228 229 • info@ilr.lu www.ilr.lu

Finalement, l'Institut ajoute une précision par rapport à la durée d'indisponibilité au sens de l'article 1 (2) (b) du projet de règlement. Le présent article se liera comme il suit :

> « *b) l'incident a entraîné une perte de disponibilité* ***d'au moins deux heures ou*** *une perte d'authenticité, d'intégrité ou de confidentialité* ***(i)*** *des données stockées, traitées, transmises ou transformées ou* ***(ii)*** *des services connexes offerts ou accessibles par l'intermédiaire d'un réseau* ***ou d'un système d'information ou d'un système biomédical*** *de l'opérateur de services essentiels,* ***à condition que cette perte de disponibilité, d'authenticité, d'intégrité ou de confidentialité ait touché*** *plus de 50 personnes au Luxembourg* ».

Quant à l'article 1er (2) (d) du projet de règlement, un opérateur s'interroge sur l'opportunité de cet article dans le cadre du milieu hospitalier et souligne les difficultés d'évaluer le préjudice corporel

L'Institut rappelle que d'un côté, le présent projet de règlement a vocation à s'appliquer à tous les services essentiels du secteur « santé » et non seulement au milieu hospitalier et d'un autre côté que cet article permet d'être en cohérence avec les autres règlements de l'Institut relatifs à d'autres secteurs.

Par ailleurs, l'Institut souligne que l'article vise le préjudice matériel d'une personne, c'est-à-dire le préjudice portant directement atteinte à son patrimoine et ainsi ne s'intéresse qu'aux conséquences matérielles d'un éventuel « préjudice corporel ».

Finalement, en ce qui concerne l'article 2 (1) du projet de règlement portant sur l'obligation d'une pré-notification, un opérateur souhaite remplacer les termes « incident détecté » par « incident confirmé ».

Dans le contexte des spécificités du secteur de santé, l'Institut entend par « incident détecté », un incident constaté par l'opérateur et pour lequel il présume que la cause provient des réseaux, systèmes d'information ou systèmes biomédicaux

L'Institut fait cette distinction spécifiquement pour le secteur de la santé, car les critères significatifs habituels (ex : décès d'une personne) peuvent s'y produire assez régulièrement sans pour autant être en relation avec un incident dont l'origine se trouve dans les réseaux, systèmes d'information ou systèmes biomédicaux.

ILR 17, rue du Fossé • Adresse postale • L-2922 Luxembourg • T +352 28 228 228 • F +352 28 228 229 • info@ilr.lu www.ilr.lu

Étant donné que le présent article a trait à une obligation d'une pré-notification et non pas à la notification finale d'un incident, il ne serait pas opportun de remplacer le terme « détecté » par le terme « confirmé ».

ILR 17, rue du Fossé • Adresse postale • L-2922 Luxembourg • T +352 28 228 228 • F +352 28 228 229 • info@ilr.lu www.ilr.lu