

PROJET DE REGLEMENT ILR/XX/X DU DD-MM-YYYY

**PORTANT DÉFINITION DE CRITÈRES ET DE SEUILS EN RELATION AVEC L'IMPACT SIGNIFICATIF SUR LE
FONCTIONNEMENT DES RÉSEAUX OU DES SERVICES DE COMMUNICATIONS ÉLECTRONIQUES.**

NISS

La Direction de l'Institut Luxembourgeois de Régulation (ci-après l'« **Institut** »),

Vu la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques et, notamment son article 27, paragraphe 1 et son article 42, paragraphe 2 ;

Vu la consultation publique nationale (CP/N23/1) relative au projet de règlement ILR/XX/X du DD-MM-YYYY portant définition de critères et de seuils en relation avec l'impact significatif sur le fonctionnement des réseaux ou des services de communications électroniques du 12 janvier 2023 au 15 février 2023 ; et

Vu le résultat de la consultation publique nationale mentionnée ci-dessus ;

Arrête :

Art. 1^{er}. (1) Les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public (ci-après les « opérateurs ») notifient à l'Institut tous les incidents de sécurité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.

(2) Un incident de sécurité est considéré comme ayant un impact significatif sur le fonctionnement des réseaux ou des services si au moins l'une des situations suivantes s'est présentée :

(a) entre 1 pour cent et 2 pour cent des utilisateurs sont concernés pendant au moins 3 heures ;

(b) entre 2 pour cent et 5 pour cent des utilisateurs sont concernés pendant au moins 2 heures ;

- (c) entre 5 pour cent et 10 pour cent des utilisateurs sont concernés pendant au moins 1 heure ;
- (d) 10 pour cent ou plus des utilisateurs sont concernés indépendamment de la durée ;
- (e) l'incident a entraîné un impact sur l'authenticité, l'intégrité ou la confidentialité (i) des réseaux, (ii) des services, (iii) des données stockées, traitées, transmises ou transformées ou (iv) d'autres services offerts ou accessibles par l'intermédiaire d'un réseau ou service du fournisseur de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public, à condition que cet impact sur l'authenticité, l'intégrité ou la confidentialité ait touché plus de 50 utilisateurs finaux au Luxembourg ;
- (f) l'incident a engendré un risque pour la sécurité ou la sûreté publique ou a entraîné un décès ;
- (g) l'incident a eu un impact sur les systèmes d'alarmes publiques (par exemple le système d'alerte national « LU-Alert ») ;
- (h) l'incident a eu un impact sur la disponibilité des services essentiels comme définis à l'annexe 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 ;
- (i) l'incident est survenu pendant des journées avec des événements critiques comme, entre autres, le jour des élections ou d'une visite étatique ;
- (j) l'incident a eu un impact sur des fonctions critiques pour la société comme, entre autres, un ministère ou une administration ;
- (k) l'incident a eu un impact sur des personnes clés comme, entre autres, des chefs d'état, des chefs de gouvernement, des parlementaires, des ministres, des ambassadeurs, et de manière générale des personnes physiques qui occupent ou se sont vu confier une fonction publique importante ;
- (l) l'incident a eu un impact transfrontalier ;
- (m) l'incident a causé un préjudice matériel d'au moins 50 000 euros à un utilisateur, malgré la mise en place par cet utilisateur de toutes les mesures nécessaires selon les règles de l'art afin d'éviter ou de réduire le préjudice résultant de l'incident ;
- (n) l'incident a eu un impact sur le fonctionnement des services d'urgence.

(3) La durée de l'incident est la période qui s'écoule entre la perturbation de la prestation du service en termes de disponibilité, d'authenticité, d'intégrité ou de confidentialité jusqu'au moment de son rétablissement.

(4) Les incidents sont à notifier à l'Institut par l'intermédiaire de la plateforme SERIMA accessible via <https://serima.lu/notification> ou bien par le biais du lien <https://niss-notification.ilr.lu> ou par un moyen automatisé à définir préalablement avec l'Institut.

Art. 2. (1) Tout incident détecté pouvant avoir un impact significatif sur le fonctionnement des réseaux ou des services doit faire l'objet d'une pré-notification à l'Institut endéans les 24 heures de sa détection et ceci selon les modalités décrites à l'article 1^{er}, paragraphe 4 du présent règlement. La pré-notification contient une estimation quant au nombre d'utilisateurs potentiellement concernés, à la durée prévisionnelle de l'incident, aux services concernés ainsi qu'une indication quant à un potentiel impact à caractère transfrontalier.

(2) Lorsqu'après une analyse interne de l'incident par le déclarant il s'avère que cet incident répond à au moins une des situations énoncées à l'article 1^{er}, paragraphe 2 du présent règlement, le déclarant fait parvenir une notification complète à l'Institut endéans un délai de 15 jours après la détection de l'incident et ceci suivant les modalités décrites à l'article 1^{er}, paragraphe 4 du présent règlement.

Cette notification complète doit au moins comprendre les informations suivantes :

- les informations de contact ;
- les services de communications électroniques impactés ;
- les informations sur l'impact de l'incident ;
- une description de l'incident ;
- la date de la première observation de l'incident ;
- la date du début de l'incident (si connue) ;
- l'impact géographique de l'incident ;
- la cause de l'incident ;
- l'information si l'incident a eu un impact sur la disponibilité, l'intégrité, la confidentialité ou l'authenticité du réseau ou service de l'opérateur.

(3) Dans le cas où des informations additionnelles sur l'incident deviendraient disponibles ultérieurement, l'opérateur procédera à une notification additionnelle après la notification complète. Cette notification additionnelle est à réaliser selon les modalités décrites à l'article 1^{er}, paragraphe 4 du présent règlement.

(4) Dans l'hypothèse où, après l'analyse interne de l'incident par le déclarant, il s'avère que l'incident, ayant déjà fait l'objet d'une pré-notification, ne répond finalement pas à au moins une des situations énumérées par l'article 1^{er}, paragraphe 2 du présent règlement, une notification complète n'est pas requise. Le déclarant en informe de suite l'Institut selon les modalités décrites à l'article 1^{er}, paragraphe 4 du présent règlement.

(5) L'opérateur partage avec l'Institut toute information divulguée par lui aux médias qui a trait à un incident ayant eu un impact significatif sur la continuité des services et réseaux.

- Art. 3.** (1) Pour les opérateurs disposant d'un réseau fixe, la méthode pour déterminer le nombre d'utilisateurs affectés par un incident est basée sur le nombre des lignes impactées par heure.
- (2) Pour le calcul du nombre total d'utilisateurs impactées, chaque ligne d'accès correspond à un utilisateur.
- Art. 4** (1) Pour les opérateurs disposant d'un réseau mobile, la méthode pour déterminer le nombre d'utilisateurs voix affectés par un incident est basée sur le nombre d'abonnements à un service voix.
- (2) La méthode pour déterminer le nombre d'utilisateurs d'un service data mobile affecté par un incident est basée sur le nombre d'abonnements à un service data mobile.
- Art. 5** Le présent règlement abroge le règlement 14/181/ILR du 28 août 2014 portant définition de critères et de seuils en relation avec l'impact significatif sur le fonctionnement des réseaux ou des services à signaler obligatoirement à l'Institut en cas d'atteinte à la sécurité ou à la perte d'intégrité de réseaux et de services de communications électroniques.
- Art. 6.** Le présent règlement sera publié au Journal officiel du Grand-Duché de Luxembourg et sur le site Internet de l'Institut.

Pour l'Institut Luxembourgeois de Régulation
La Direction

Michèle Bram
Directrice adjointe

Camille Hierzig
Directeur adjoint

Luc Tapella
Directeur