CIRCULAIRE N° 2026-078

CIRCULAIRE

AUX ADMINISTRATIONS COMMUNALES,
AUX SYNDICATS DE COMMUNES,
AUX OFFICES SOCIAUX,
AUX AUTRES ÉTABLISSEMENTS PUBLICS PLACÉS SOUS LA SURVEILLANCE DES COMMUNES

Loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité (loi « NIS 2 ») : implications pour le secteur communal et responsabilités des élus – Séances d'information

Luxembourg, le 21 septembre 2026

Madame la Bourgmestre, Monsieur le Bourgmestre,
Madame la Présidente, Monsieur le Président,

Faisant suite à la circulaire n° 2025-062 du 10 septembre 2025, nous tenons à vous informer que la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité (ci-après « loi NIS 2 ») est entrée en vigueur le 10 mai 2026.

Pour rappel, elle a pour objet de transposer la 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), appelée communément « directive NIS 2 ».

Les obligations qui en résultent pour le secteur communal ont déjà été présentées lors de la conférence « *Wéi digital resilient ass de Gemengesecteur ?* », qui avait été organisée le 7 mai 2024 à Bissen, de même que lors de l'évènement « Transposition de la Directive NIS 2 : soutien offert au secteur communal », qui avait été organisé le 12 juin 2025 à Itzig et dont l'objectif était de mettre l'accent davantage sur les mesures concrètes à prendre et les services proposés aux communes par le Luxembourg House of Cybersecurity (LHC).

Finalement, les entités du secteur communal ont été informées sur les implications de la directive NIS 2 par la circulaire ministérielle n°2025-062 du 10 septembre 2025, alors que la transposition était en cours.

La présente circulaire vise à rappeler le contexte de la loi NIS 2 (1) et de vous communiquer des informations complémentaires, les implications sur les entités du secteur communal (2) et les informations et ressources disponibles pour accompagner leur mise en conformité, **dont notamment l'organisation de deux séances d'information** (3).

1. Contexte de la loi NIS 2

La loi NIS 2 est entrée en vigueur le 10 mai 2026 au Luxembourg. Depuis cette date, les entités essentielles et importantes sont soumises à différentes obligations telles que la mise en place de mesures de cybersécurité, la protection de leurs systèmes d'informations et la sécurisation de leur chaine d'approvisionnement.

Elles sont également tenues de notifier tous les incidents importants ayant un impact sur les systèmes d'informations dans un délai de 24 heures à l'autorité compétente.

Enfin, la loi NIS 2 renforce la responsabilisation des organes de direction. Les dirigeants sont tenus responsables d'intégrer la cybersécurité dans la gouvernance de l'organisation. Ils doivent donc avoir les connaissances nécessaires afin de comprendre les risques de cybersécurité et d'approuver les mesures de sécurité à mettre en place. Au niveau du secteur communal, cela incombe au collège des bourgmestre et échevins, au bureau ou président.

2. Implications pour les entités du secteur communal

Les administrations communales en tant qu'entités de l'administration publique ont les obligations suivantes :

2.1. Auto-enregistrement auprès de l'ILR

La loi NIS 2 s'applique à toutes les entités de l'administration publique et, selon les critères définis à l'article 2, point 34°, les entités du secteur communal tombent sous cette définition. Ainsi, ces entités sont directement visées en tant qu'entités essentielles (indépendamment de leur taille) par les dispositions applicables[1].

Selon l'article 11, paragraphe 4, de la loi NIS 2, les entités essentielles et importantes sont obligées de communiquer aux autorités compétentes un certain nombre d'informations et ceci dans un délai de deux mois à compter de l'entrée en vigueur de la loi. Le but est de recueillir des informations complémentaires nécessaires au suivi des entités sous NIS 2, notamment des informations de contact, des informations sur les secteurs et sous-secteurs d'activité, la taille de l'entité, etc.

En tant qu'entités essentielles du secteur « Administration publique », les entités du secteur communal ont donc eu l'obligation de s'enregistrer elles-mêmes auprès de l'ILR pour le 10 juillet 2026 en utilisant le formulaire d'auto-enregistrement disponible sur le site web[2] de l'Institut.

2.2. Notifications d'incidents

Depuis l'entrée en vigueur de la loi NIS 2, les entités du secteur communal sont tenues de notifier tout incident important dans un délai de 24 heures après détection à l'ILR (notification préliminaire)[3]. La notion d'incident[4] est volontairement large : elle englobe aussi bien les cyberattaques que les erreurs humaines, les défaillances techniques ou encore les évènements physiques susceptibles d'affecter les systèmes d'informations et les données.

Conformément à l'article 14, paragraphe 3, de la loi NIS 2, un incident est considéré comme important :

[1] Article 11 (1), point 4° de la loi NIS 2
[2] https://www.ilr.lu/secteurs-activites/niss/auto-enregistrement/
[3] Article 14 (4) de la loi NIS 2
[4] Article 2, point 5° de la loi NIS 2

- S'il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée ;
- S'il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

Afin de faciliter la notification d'incident, l'ILR a mis en place la plateforme serima.lu permettant de notifier les incidents importants dans les délais prévus par la loi.

2.3. Mise en place de mesures de sécurité adéquates

Différentes mesures de sécurité doivent être mises en place pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que les entités utilisent dans le cadre de leurs activités afin d'éliminer ou de réduire les impacts sur la population en cas d'incidents.

Ces mesures comprennent au moins (art. 12, paragraphe 1er, de la loi NIS 2) :

- les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;
- la gestion des incidents ;
- la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises ;
- la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ;
- la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
- des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
- les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité ;
- des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
- la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;
- l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

2.4. Notification annuelle des mesures de sécurité à l'ILR

Afin de pouvoir analyser le niveau de cybersécurité des entités, l'ILR demande aux entités essentielles de soumettre annuellement :

- Leur description des mesures en place reflétant les mesures de cybersécurité en place ;
- Une analyse des principaux scénarios de risques cyber, sous forme de questionnaire à choix multiples ;
- Un plan d'action pluriannuel détaillant les mesures prévues afin d'assurer un niveau de cybersécurité élevé.

Un règlement ILR, qui sera publié, en précisera les modalités.

2.5. Responsabilités du collège des bourgmestre et échevins

Au-delà des obligations opérationnelles, la loi NIS 2 introduit un changement majeur en matière de responsabilités. Les organes de direction, qui sont dans le secteur communal le collège des bourgmestre et échevins, se voient attribuer des obligations et responsabilités directes par la loi NIS 2.

Ces obligations impliquent de devoir s'informer, se former, former leurs équipes, ainsi qu'approuver et superviser la mise en place des mesures de gestion des risques en matière de cybersécurité de l'entité.

La cybersécurité devient ainsi un véritable enjeu de gouvernance et un sujet stratégique au plus haut niveau de l'entité.

Conformément à l'article 13 de la loi NIS 2, les membres des organes de direction doivent :

- approuver les mesures de gestion des risques en matière de cybersécurité et superviser leur mise en œuvre, ce qui inclut la validation des résultats des évaluations de risques ainsi que des plans de remédiation associés ;
- suivre régulièrement une formation afin d'acquérir les connaissances et compétences suffisantes pour évaluer les risques en cybersécurité, comprendre les impacts sur les services fournis, prendre des décisions éclairées, notamment pour la gestion des ressources, et assumer pleinement leurs responsabilités ; et
- veiller à ce que des formations similaires soient régulièrement proposées aux membres du personnel, afin d'acquérir les bonnes pratiques pour la gestion des risques et garantir une formation continue et adaptée à tous les niveaux de l'organisation.

3. Information et accompagnement

3.1 Séances d'information

Sur l'initiative du SYVICOL et du ministère des Affaires intérieures, deux séances d'information sont prévues.

Ce sera l'occasion pour l'ILR de présenter plus en détail les implications de la loi NIS 2 pour le secteur communal et les nouvelles responsabilités et obligations et matière de cybersécurité.

En outre, le Luxembourg House of Cybersecurity (LHC) y présentera son rôle et ses missions, ainsi que les démarches à suivre en cas d'incident.

Finalement, la commune de Hesperange donnera un aperçu sur ses initiatives pratiques dans le cadre de la mise en œuvre de la loi NIS 2.

Les séances seront clôturées par un échange convivial autour d'un verre de l'amitié.

Elles auront lieu :

- **le mardi 6 octobre 2026 à 16h00 au siège de l'ILR, 17 Rue du Fossé, Luxembourg ; (inscription :** https://pretix.eu/ILR-NIS2-information-session/9y9eq/)
- **le lundi 19 octobre 2026 à 16h00 dans la salle « Al Schoul », 72, Rte de Luxembourg, Schieren (inscription :** https://pretix.eu/ILR-NIS2-information-session/gv8v9/)

Les participants sont invités à s'inscrire au moins 5 jours à l'avance pour la réunion de leur choix moyennant les liens indiqués.

3.2 Ressources et support

Plusieurs institutions sont à disposition pour accompagner les entités du secteur communal dans la mise en œuvre des exigences NIS 2 :

- L'ILR organise régulièrement des séances d'informations NIS 2[5].
- Votre prestataire de produits et services informatiques dans la mesure où ces services tombent dans le champ d'application de la directive.
- Sont compétents pour assister les communes dans la gestion des incidents de cybersécurité :
    1. Le *Computer Incident Response Center Luxembourg* (CIRCL), un service de la *Luxembourg House of Cybersecurity* (LHC),
    2. respectivement pour les communes désignées comme entités critiques en vertu de la loi du sur la résilience des entités critiques (REC)[6], le Haut-Commissariat à la protection nationale dans sa fonction de CERT Gouvernemental (GOVCERT) ;

  CIRCL est aussi compétent en matière de divulgation des vulnérabilités (https://circl.lu/pub/coordinated-vulnerability-disclosure/).
- Le *National Cybersecurity Competence Center* (NC3), un service de la *Luxembourg House of Cybersecurity* (LHC), met à disposition des ressources et des outils pour accompagner les communes et syndicats intercommunaux dans la gouvernance de la sécurité de l'information (des informations complémentaires sur les services et ressources du NC3 peuvent être consultées sur le site https://nc3.lu/).
- Le NC3, en collaboration avec le SIGI et le SYVICOL, a notamment mis en place une plateforme de formation en ligne destinée à sensibiliser aux bonnes pratiques de cybersécurité et à fournir des outils efficaces en la matière. Ces formations interactives, qui peuvent être suivies à tout moment, sont offertes gratuitement par le NC3 et s'adressent tant aux agents du secteur communal qu'aux responsables politiques. Pour davantage d'informations, veuillez consulter la circulaire y relative.
- L'institut national d'administration publique (INAP) organise également des formations relatives à la sécurité de l'information qui s'adressent aux agents communaux. Ces formations, élaborées en concertation avec le Haut-Commissariat à la protection nationale (HCPN) dans sa fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI), comprennent notamment une initiation à la sécurité de l'information et une Cybersecurity Escape Room. Des formations à destination des cadres dirigeants et des agents impliqués dans la cybersécurité seront également intégrées au catalogue de l'INAP.[7]

Par ailleurs, le HCPN, dans sa fonction d'ANSSI, met à disposition un ensemble complet de politiques et lignes directrices en matière de sécurité de l'information ainsi que des guidances d'implémentation : Documentation HCPN-ANSSI Luxembourg.

[5] Un enregistrement d'une séance d'information peut être trouvé ici: Sessions d'informations - ILR
[6] https://www.chd.lu/fr/dossier/8307
[7] Des places restent disponibles notamment pour la formation "Sécurité de l'information : Comprendre les risques, adopter les bonnes pratiques (e-Learning)"(https://govcampus.public.lu/trainings/00027764)

Finalement, nous vous saurions gré de bien vouloir vous adresser aux institutions suivantes pour toute question ayant trait à la présente circulaire :

Institution	**Domaine de responsabilité**	**Adresse mail**
ILR	Autorité compétente NIS 2	nis2@ilr.lu
CIRCL	Gestion des incidents de cybersécurité	info@circl.lu
GOVCERT	Gestion des incidents de cybersécurité (Communes désignées comme entités critiques selon REC)	info@govcert.etat.lu
NC3	Analyse de risques et résilience (formations MONARC et ROOM#42)	info@nc3.lu
INAP	Formations	info@inap.etat.lu
ANSSI	Politiques et lignes directrices en matière de sécurité de l'information	info@anssi.etat.lu
LHC	Ecosystème cybersécurité luxembourgeois (pour tout besoin de prestation ou service fourni par des acteurs du marché national)	info@lhc.lu *(https://cybersecurity.lu/)*

Veuillez agréer, Madame la Bourgmestre, Monsieur le Bourgmestre, Madame la Présidente, Monsieur le Président, l'assurance de notre parfaite considération.

Le Ministre des Affaires intérieures,

Léon Gloden

Le Président du SYVICOL,

Emile Eicher