Luxembourg, le 10 septembre 2025

**Circulaire n° 2025-062**

# Circulaire

aux administrations communales,
aux syndicats de communes,
aux offices sociaux,
aux autres établissements publics placés sous la surveillance des communes

Objet : Transposition de la directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne (directive dite « SRI 2 » ou « NIS 2 »)

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

Dans le cadre de la mise en œuvre de la directive NIS2, je tiens à vous informer des implications pour les communes, les syndicats de communes, les offices sociaux et les autres établissements publics placés sous la surveillance des communes (entités du secteur communal), qui seront soutenus dans leurs tâches par l'autorité compétente, c-à-d l'Institut luxembourgeois de régulation (ILR) et les autres institutions actives dans le domaine de la cybersécurité au niveau national.

## 1. Contexte et objectifs de la directive NIS 2

La directive NIS 2 vise à renforcer la cybersécurité dans toute l'Union européenne. Elle remplace la directive NIS 1 de 2016 et harmonise les exigences à travers les États membres en fixant des règles communes pour assurer un niveau approprié de sécurité des réseaux et systèmes d'information. Les entités du secteur communal, en tant qu'entités de l'administration publique au niveau local et, partiellement, en tant qu'entités prestant des services hautement critiques (fourniture et distribution d'eau potable ; collecte, évacuation et traitement des eaux usés), respectivement en tant qu'entités prestant des services critiques (gestion des déchets), sont désormais concernées.

## 2. Implications pour les entités du secteur communal

### 2.1. Pourquoi les entités du secteur communal sont-elles directement concernées ?

La directive NIS 2 et le projet de loi n° 8364[1] définissent ce qu'il y a lieu d'entendre par « entité de l'administration publique » et selon les critères établis, qui sont à remplir cumulativement, 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.

### 2.2. Obligations pour les entités du secteur communal

Les entités du secteur communal seront notamment tenues de prendre les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité de leurs réseaux et des systèmes d'information. Ces mesures doivent garantir un niveau de sécurité adapté au risque, en tenant compte de l'état des connaissances et, le cas échéant, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre.

Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir compte du degré d'exposition aux risques et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

Ces mesures devront être fondées sur une approche « tous risques » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent notamment :

- La mise en place d'une gouvernance de la cybersécurité, comprenant notamment l'implication et la formation continue des membres des organes exécutifs des entités du secteur communal, l'attribution formelle des responsabilités en matière de cybersécurité et l'intégration de la cybersécurité dans la gestion des projets, etc. ;
- L'analyse et l'évaluation des risques liés à la cybersécurité pesant sur les réseaux et systèmes d'information ;
- La gestion des incidents de cybersécurité, y compris la notification à l'autorité compétente (ILR) des incidents ayant un impact significatif sur la sécurité des services essentiels, selon les modalités et les délais définis ;
- L'assurance de la continuité des services essentiels et la gestion de crises ;
- La définition et la mise en œuvre des politiques en matière de gestion de la cybersécurité telles que la sécurité des ressources humaines, la gestion des identités et des accès ; le recours systématique à l'authentification forte, la gestion des actifs, la cryptographie, etc. ;
- La sécurité de la chaîne d'approvisionnement y compris les aspects liés à la sécurité concernant les relations entre les communes 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 la gestion et la divulgation des vulnérabilités ;
- La sensibilisation des agents communaux aux bonnes pratiques de cybersécurité et intégration de la cybersécurité dans les programmes de formation continue ;

[1] https://www.chd.lu/fr/dossier/8364

- La notification sans retard des incidents (événements compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles importants) à l'ILR et le cas échéant les destinataires des services concernés.

## 3. Se préparer dès maintenant

La transposition de la directive NIS 2 en droit national est actuellement en cours par le biais du projet de loi n° 8364).

Nous recommandons vivement aux entités du secteur communal d'entamer dès à présent les démarches de préparation :

- Répertorier les activités essentielles et les systèmes qui les supportent ;
- Initier une autoévaluation de maturité en cybersécurité ;
- Sensibiliser le collège échevinal et les agents aux risques cyber ;
- Mettre en place un processus de gestion des incidents ;
- Suivre les recommandations de l'ILR et d'autres acteurs appropriés.

### 3.1. 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 ;
- 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)[2], 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. En particulier, l'outil d'analyse de risque MONARC (intégré également dans la plateforme SERIMA de l'ILR), pour lequel des formations sont régulièrement proposées ou encore le « *simulateur de cyber crise* », la ROOM#42, pour se préparer à la bonne gestion d'incidents et devenir plus résilient. (des informations complémentaires sur les services et ressources du NC3 peuvent être consultées sur le site https://nc3.lu/) ;
- L'institut national d'administration publique (INAP) organise également des formations relatives à la sécurité de l'information. Ces formations, élaborées en concertation avec le Haut-

[2] https://www.chd.lu/fr/dossier/8307

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.

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.

Dorénavant, le LHC et l'ILR ont le plaisir d'inviter à leur prochaine séance d'information sur la directive NIS 2. Cette séance aura lieu le 23 septembre 2025 de 10h00 à 12h00 et vous pouvez dès lors vous inscrire à travers le formulaire en ligne suivant : https://pretix.eu/ILR-NIS2/nyzxp/. Les détails de l'organisation de cette séance seront communiqués ultérieurement.

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 | 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 fournit par des acteurs du marché nationale) | info@lhc.lu *(https://cybersecurity.lu/)* |

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

Le Ministre des Affaires intérieures

Léon Gloden