CENTRE FOR
CYBER SECURITY
BELGIUM

GUIDE SUR LES NOTIFICATIONS D'INCIDENTS NIS

LES OPERATEURS DE SERVICES ESSENTIELS (OSE)

CENTRE POUR LA
CYBERSECURITE BELGIQUE
Rue de la Loi, 16
1000 Bruxelles

nis@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

Avertissement :

Le présent guide vise à répondre aux principales questions relatives à la notification des incidents NIS des opérateurs de services essentiels en Belgique.

Celui-ci n'est toutefois pas exhaustif et ne dispense pas les opérateurs de services essentiels de l'examen des dispositions légales générales ou sectorielles pertinentes.

Table des matières

A. Lexique **3**

B. Notification des incidents NIS par les opérateurs de services essentiels (OSE) **6**

1. Quels événements doivent être notifiés obligatoirement par un OSE ? *6*

2. Dans quel délai un incident doit-il être notifié ? *7*

3. A qui l'OSE doit-il notifier l'incident ? *7*

4. Comment l'OSE doit-il notifier l'incident ? *8*

5. Quelles informations l'OSE doit-il transmettre ? *10*

6. Quelles sont les différentes étapes de notification d'un incident ? *10*

7. Quelles sont les règles relatives à la confidentialité des informations liées à un incident NIS ? *12*

8. Quelles sont les autres obligations imposées à l'OSE suite à la notification d'un incident ? *13*

9. Que faire si un incident NIS est également une violation de données à caractère personnel ? *13*

10. Quels évènements peuvent être notifiés à titre volontaire ? *14*

C. Annexe I de la loi NIS **16**

D. Sanctions **18**

E. Assistance technique **19**

F. Points de contact NIS **19**

G. Références légales **23**

A. Lexique

« Arrêté royal NIS » *: l'arrêté royal du 12 juillet 2019 portant exécution de la loi NIS, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (M.B., 18 juillet 2019, p. 72187 et s).*

« Autorité sectorielle »*: l'autorité publique compétente pour la désignation et le contrôle des OSE dans l'un des secteurs repris à l'annexe I de la loi NIS (Energie, Transports, Finances, Santé, Eau potable et Infrastructures numériques).*

« Centre pour la Cybersécurité Belgique (CCB) » : *administration fédérale sous l'autorité du Premier Ministre et créée par l'arrêté royal du 10 octobre 2014 (M.B., 21 novembre 2014, p. 91395 et s.).*

« Centre de crise national (NCCN) » : *Direction générale du Service public fédéral Intérieur, créé par l'arrêté royal du 18 avril 1988 (M.B., 4 mai 1988, p. 6408 et s).*

« Computer Emergency Response Team (CERT.be)» : *service opérationnel de réponse aux incidents de sécurité informatique du Centre pour la Cybersécurité Belgique.*

« CSIRT national » *: le Centre national de réponse aux incidents de sécurité informatique, à savoir le Centre pour la Cybersécurité Belgique (CCB).*

« CSIRT sectoriel » *: le centre sectoriel de réponse aux incidents de sécurité informatique [non obligatoire].*

« Gestion d'incident » : *toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident.*

« Incident » : *tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information.*

« Loi NIS» *: la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (M.B., 3 mai 2019, p. 42857 et s).*

« Opérateur de services essentiels » (OSE) *: une entité publique ou privée active en Belgique dans l'un des secteurs repris à l'annexe I de la loi NIS (Energie, Transports, Finances, Santé, Eau potable et Infrastructures numériques) et qui a été désignée comme telle par l'autorité sectorielle compétente (art. 6, 11° de la loi NIS).*

« Opérateur de services essentiels potentiel » *: une entité publique ou privée active en Belgique dans l'un des secteurs repris à l'annexe I de la loi NIS, mais qui n'a pas été désignée comme opérateur de services essentiels.*

« Plate-forme de notification » *: la plate-forme de notification d'incidents visée à l'article 31 de la loi NIS.*

« Point de contact pour la sécurité des systèmes et réseaux d'information » *: le point de contact désigné par l'opérateur de services essentiels et qui exerce la fonction de point de contact vis-à-vis du CCB, du NCCN et de l'autorité sectorielle pour toute question liée à la sécurité des réseaux et des systèmes d'information dont sont tributaires les services essentiels fournis.*

« Politique de sécurité des systèmes et réseaux d'information » *(P.S.I.) : un document visé à l'article 21, § 1er , reprenant les mesures de sécurité des réseaux et des systèmes d'information adoptées par un opérateur de services essentiels.*

« Règlement UE 2016/679 » *: le Règlement européen 2016/679 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 (Règlement général sur la protection des données « RGPD »).*

« Réseau et système d'information » :

a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques ;
b) tout dispositif, tout ensemble de dispositifs interconnectés ou apparentés, de manière permanente ou temporaire, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou

mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel ;
c) ou les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b), en vue de leur fonctionnement, utilisation, protection et maintenance.

« Risque » : *toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information.*

« Sécurité des réseaux et des systèmes d'information » : *la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.*

B. Notification des incidents NIS par les opérateurs de services essentiels (OSE)

1. Quels événements doivent être notifiés obligatoirement par un OSE ?

a) L'OSE (qui n'est pas supervisé par la Banque nationale de Belgique « BNB ») notifie **tous les incidents ayant un impact** sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les service(s) essentiel(s) qu'il fournit[1].

La loi NIS prévoit la possibilité de fixer, par arrêté royal, des niveaux d'incidence et/ou des seuils pour la notification des incidents ou encore différentes catégories de notification en fonction du degré d'impact de l'incident[2]. A ce jour, de tels arrêtés royaux n'ont toutefois pas été adoptés.

b) L'OSE supervisé par la BNB notifie **tous les incidents ayant un impact significatif** sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit.

La BNB est chargée de déterminer cet impact significatif[3].

Un incident est « tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information »[4].

La disponibilité est l'aptitude d'un système d'information à être accessible et utilisable à la demande d'une entité autorisée. Il s'agit de garantir le fonctionnement normal d'un système d'information.

---

[1] Art. 24, § 1er de la loi NIS prévoit la notification, sans retard, de tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels que l'opérateur fournit. L'art. 24, § 3 précise qu'en l'absence de niveaux d'incidence et/ou de seuils visés au paragraphe 2, l'opérateur notifie tous les incidents ayant un impact sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit.
[2] Art 24, § 2 et § 3 de la loi NIS.
[3] Art. 26, § 2 de la loi NIS.
[4] Art. 6, 13°, de la loi NIS.

La confidentialité est l'aptitude d'un système d'information à ne pas permettre l'accès à ses données à des personnes ou entités non autorisées. Il s'agit d'éviter que les informations tombent entre des mains malveillantes ou soient rendues publiques sans le consentement du responsable du système d'information.

L'intégrité est l'aptitude d'un système d'information à ne pas être altéré par des entités non autorisées. Il s'agit de se prémunir contre une modification illégitime et nuisible du système d'information.

L'authenticité est l'aptitude d'un système d'information à confirmer qu'il est ce qu'il prétend être. Il s'agit d'être certain que les données proviennent bien d'un système d'information déterminé.

2. Dans quel délai un incident doit-il être notifié ?

L'OSE doit notifier l'incident **sans retard**[5], c'est-à-dire le plus rapidement possible.

L'OSE ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification. Lorsque les informations en sa possession lui permettent de savoir qu'il s'agit d'un incident soumis à notification, il doit le faire sans attendre[6].

3. A qui l'OSE doit-il notifier l'incident ?

a) L'OSE (qui n'est pas supervisé par la BNB) doit notifier simultanément l'incident à trois autorités[7] :

- le Centre pour la Cybersécurité Belgique (CCB) ;
- le Centre de Crise national (NCCN) ;
- l'autorité sectorielle et/ou à son CSIRT sectoriel.

[5] Art. 24, § 1er, de la loi NIS.
[6] Art. 25, al. 2, de la loi NIS.
[7] Art. 25 de la loi NIS.

En pratique, la notification simultanée s'accomplit en une seule démarche aux trois autorités via l'utilisation de la plate-forme de notification NIS.

b) L'OSE supervisé par la BNB doit notifier l'incident uniquement à la BNB, selon les modalités fixées par celle-ci.

Si la BNB impose à l'OSE d'utiliser la plate-forme de notification, la notification est simultanément aussi faite au CCB et au NCCN. Si la BNB n'impose pas l'utilisation de la plate-forme de notification, la BNB transmettra elle-même la notification, sans retard, au CCB et au NCCN[8].

Cette exception résulte du fait que certains établissements financiers sont déjà soumis à des obligations de notification sectorielles au niveau européen vis-à-vis de la Banque Centrale européenne.

4. Comment l'OSE doit-il notifier l'incident ?

a) pour les OSE, sauf ceux supervisés par la BNB :

La notification doit être réalisée via ***la plate-forme de notification NIS***[9] : https://nis-incident.be

La plate-forme est accessible par le biais d'internet au moyen d'une connexion sécurisée et l'utilisation d'une clé d'identification unique à chaque OSE (login/nom d'utilisateur et mot de passe)[10].

b) pour les OSE supervisés par la BNB :

La BNB peut demander aux OSE d'utiliser la plate-forme de notification NIS ou d'autres outils de notification.

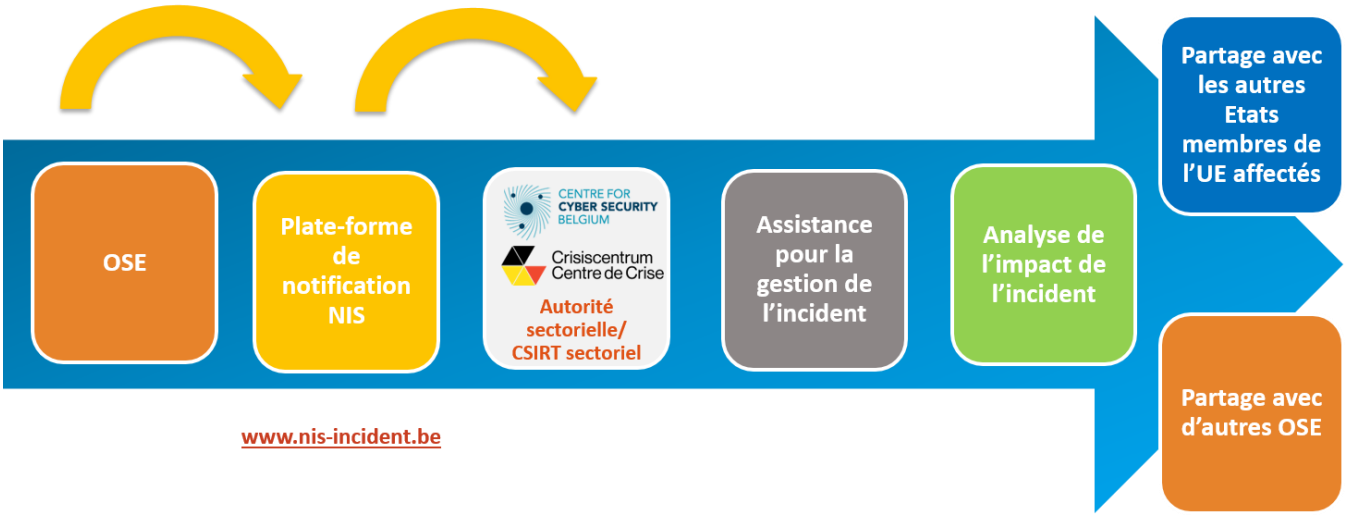
---

[8] Art. 26, § 2 de la loi NIS.
[9] Voy. art. 31, § 1er, de la loi NIS et art. 8 de l'AR NIS.
[10] Art. 7 de l'AR NIS.

CSIRTs NETWORK

NIS COOPERATION GROUP

Notification des incidents NIS
(sauf OSE supervisés par la BNB)



www.nis-incident.be

EUROPEAN CENTRAL BANK
EUROSYSTEM

CSIRTs NETWORK

NIS COOPERATION GROUP

Notification des incidents NIS
OSE supervisés par la BNB

www.nis-incident.be

En cas d'indisponibilité de la plate-forme de notification NIS, l'OSE doit notifier l'incident via les modalités reprises sur le site du CCB (https://cert.be/fr/signaler-un-incident).

5. Quelles informations l'OSE doit-il transmettre ?

L'OSE utilisera le formulaire de notification d'incident, repris sur la plate-forme de notification NIS : https://nis-incident.be

La notification contient toutes les informations disponibles permettant de déterminer la nature, les causes, les effets et les conséquences de l'incident[11] :

a) le nom et les coordonnées de l'opérateur et le service qu'il fournit ;
b) la date et le moment où l'incident s'est produit ;
c) la durée de l'incident ;
d) l'étendue géographique de l'incident et son caractère éventuellement transfrontalier;
e) le nombre d'utilisateurs concernés ;
f) les informations sur la nature de l'incident ;
g) la portée de l'impact de l'incident, notamment sur les activités sociales et économiques ;
h) l'importance des systèmes ou de l'information concernée ;
i) l'impact de l'incident sur des organisations internationales installées en Belgique ;
j) les actions entreprises ;
k) la description de la situation actuelle.

6. Quelles sont les différentes étapes de notification d'un incident ?

La procédure de notification peut s'accomplir en plusieurs étapes :

a) ***Une notification initiale*** doit être effectuée, sans retard, même si l'OSE ne dispose pas encore de toutes les informations pertinentes. Le but de cette notification initiale est d'attirer

[11] Art. 8, § 1er, de l'AR NIS.

l'attention du CCB, de l'autorité sectorielle ou de son CSIRT sectoriel, et du NCCN sur l'incident et de ses possibles conséquences.

b) ***Des notifications complémentaires***[12] doivent être envoyées périodiquement ou dès que l'OSE dispose de nouvelles informations. Le but de ces notifications complémentaires est de mettre à jour le CCB, l'autorité sectorielle ou son CSIRT sectoriel, et le NCCN sur le statut de l'incident. L'OSE crée alors une nouvelle notification sur la plate-forme, en y ajoutant seulement les données nouvelles ainsi que le numéro de référence de la notification initiale.

c) ***Un éventuel rapport final*** (à la demande de l'une des autorités précitées) reprenant toutes les informations envoyées au CCB, à l'autorité sectorielle ou son CSIRT sectoriel, et au NCCN. Le but de ce rapport final est de donner une vue d'ensemble de l'incident et de pouvoir en tirer des conclusions.

L'OSE doit tenir informé le CCB et l'autorité sectorielle, ou le cas échéant le CSIRT sectoriel, de l'évolution de l'incident ainsi que des actions de remédiation entreprises.

Lorsque l'OSE n'est pas en mesure de fournir toutes les informations reprises dans le formulaire à l'aide des éléments en sa possession, il complète la notification initiale via la plate-forme de notification dès que les informations manquantes sont disponibles[13].

Il fait de même lorsque de nouvelles informations sont connues ou lorsque des développements importants surviennent[14].

A la demande du CCB, du NCCN, de l'autorité sectorielle ou de son CSIRT sectoriel, l'OSE notifie via la plate-forme de notification une mise à jour du formulaire de notification (« rapport final ») retraçant la gestion de l'incident de sa découverte à sa clôture et reprenant toutes les informations reprises dans le formulaire de notification[15].

---

[12] Art. 8, § 3 de l'AR NIS
[13] Art. 8, § 2, de l'AR NIS.
[14] Art. 8, § 3, de l'AR NIS.
[15] Art. 8, § 4, de l'AR NIS.

Les notifications complémentaires (visées à l'article 8, § 3 de l'AR NIS) faites par l'OSE suite à la prise de connaissance de nouvelles informations ou à la survenance de développements importants relatifs à l'incident seront réalisées via la plate-forme de notification.

7. Quelles sont les règles relatives à la confidentialité des informations liées à un incident NIS ?

L'OSE et ses sous-traitants limitent l'accès aux informations relatives aux incidents, au sens de la loi NIS, aux seules personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la loi NIS[16].

Cette règle vaut également pour le CCB (CSIRT national), le NCCN, l'autorité sectorielle et l'éventuel CSIRT sectoriel.

Les membres du personnel de l'OSE et ses sous-traitants sont tenus au secret professionnel en ce qui concerne les informations en rapport avec un incident NIS[17].

Les informations fournies au CCB, au NCCN et à l'autorité sectorielle par un OSE peuvent être échangées avec des autorités d'autres Etats membres de l'Union européenne et avec d'autres autorités belges lorsque cet échange est nécessaire à l'application de dispositions légales.

Cette transmission d'informations se limite toutefois à ce qui est pertinent et proportionné à l'objectif de cet échange, dans le respect du Règlement UE 2016/679, de la confidentialité des informations concernées, de la sécurité et des intérêts commerciaux de l'OSE[18].

La confidentialité des informations qui se trouvent sur la plate-forme de notification est également garantie par l'article 458 du Code pénal, par l'arrêté royal du 2 octobre 1937 portant le statut des agents de l'Etat, par l'article 17, 3°, a) de la loi du 3 juillet 1978 relative aux contrats de travail, par

[16] Art. 9, § 1er, de la loi NIS.
[17] Art. 9, § 2, de la loi NIS.
[18] Art. 9, § 3, de la loi NIS.

l'article 23 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges et par les autres dispositions pertinentes applicables.

8. Quelles sont les autres obligations imposées à l'OSE suite à la notification d'un incident ?

L'OSE qui est touché par un incident est obligé de gérer l'incident et de prendre les mesures réactives afin de le résoudre. La gestion de l'incident demeure de la responsabilité de l'OSE[19].

L'OSE doit examiner les incidents ou évènements suspects qui lui sont notifiés par le CCB, l'autorité sectorielle ou le NCCN[20].

Le CCB, l'autorité sectorielle ou son CSIRT sectoriel et le NCCN peuvent demander à l'OSE des informations complémentaires relatives aux notifications qu'il a effectuées.

Les OSE supervisés par la BNB gèrent l'incident tenant compte des dispositions légales et des instructions qui leurs sont rendus applicables par la BNB et/ou la Banque centrale européenne.

Lorsque les circonstances le permettent, le CCB fournit à l'OSE qui est à l'origine de la notification toutes les informations utiles au suivi de sa notification, et le cas échéant toutes les informations qui pourraient contribuer à une gestion efficace de l'incident[21].

9. Que faire si un incident NIS est également une violation de données à caractère personnel ?

[19] Art. 28, § 1er, de la loi NIS.
[20] Art. 28, § 2, de la loi NIS.
[21] Art. 10 de l'AR NIS.

En fonction des informations introduites, l'OSE recevra un message standard l'informant de son obligation de notifier les éventuelles violations de données à caractère personnel[22] à l'une des « autorités de contrôle » via les outils de notification appropriés (par exemple : www.autoriteprotectiondonnees.be/formulaire-notification-de-fuites-de-donnees).

Règles particulières relatives aux données à caractère personnel

Les traitements de données à caractère personnel effectués par un OSE dans le cadre de la loi NIS peuvent éventuellement déroger aux articles 12 à 22 du Règlement général sur la protection des données « RGPD » (*Règlement (UE) 2016/679 Chapitre III - Droits de la personne concernée*). L'exemption vaut, sous réserve du principe de proportionnalité et le cas échéant de minimisation des données, pour toutes les catégories de données à caractère personnel, dans la mesure où le traitement de ces données n'est pas étranger à la finalité du traitement (par exemple, la notification d'un incident) et est nécessaire pour cette finalité[23].

Les données (en ce compris les données à caractère personnel) ne doivent pas être conservées par l'OSE plus longtemps que nécessaire pour la poursuite des objectifs de la loi avec une durée maximale de conservation ne pouvant excéder la durée du délai de prescription des infractions éventuelles visées aux articles 51, § 1 et 52, § 2 de la loi NIS[24].

10. Quels évènements peuvent être notifiés à titre volontaire ?

[22] Art. 33, 1er alinéa, du règlement UE 2016/679 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.
[23] Art. 71, § 2 et § 4 de la loi NIS.
[24] Art. 71, § 5, de la loi NIS.

Un « opérateur de services essentiels potentiels »[25] peut notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'il fournit.

Cette notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de la notification des obligations auxquelles elle n'aurait pas été soumise si elle n'avait pas procédé à ladite notification[26].

Lors du traitement des notifications, le CCB, l'autorité sectorielle ou son CSIRT sectoriel, et le NCCN peuvent donner la priorité aux notifications obligatoires imposées par la loi NIS par rapport aux notifications volontaires.

Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile à charge des autorités susmentionnées.

Les notifications volontaires sont adressées directement au CCB par l'OSE potentiel via les modalités prévues sur le site du Centre pour la Cybersécurité Belgique (service CERT.be)[27] : https://cert.be/fr/signaler-un-incident

[25] entités publiques ou privées actives en Belgique dans l'un des secteurs repris à l'annexe I de la loi NIS : Energie, Transports, Finances, Santé, Eau potable et Infrastructures numériques, mais qui n'ont pas été désignés comme OSE (ex : un nouvel opérateur ou un opérateur qui se trouve en dessous des seuils ou niveaux d'incidence d'identification fixés par l'autorité sectorielle).
[26] Art. 30, § 1er, de la loi NIS.
[27] Art. 12 de l'AR NIS.

C. Annexe I de la loi NIS

Secteur, sous-secteur, type d'OSE		
Secteur	**Sous-secteur**	**Type**
Energie	a) Electricité b) Pétrole c) Gaz	Ex: gestionnaire de réseau de distribution au sens de l'article 2, 11° de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité.
Transports	a) Transport aérien b) Transport ferroviaire c) Transport par voie d'eau d) Transport routier	Ex: entreprise ferroviaire au sens de l'article 3, 27° du Code ferroviaire. Entité gestionnaire des ports au sens de l'article 5, point 7) de la loi du 5 février 2007 relative à la sûreté maritime.
Finances	a) Etablissements financiers b) Plates-formes de négociation financière	Etablissements de crédit, contreparties centrales, autres établissements financiers Opérateurs de plate-forme de négociation financière
Santé	Etablissements de soins de santé (y compris les hôpitaux et les cliniques privées)	Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement

		européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers.
Eau potable		Fournisseurs et distributeurs d'eau destinée à la consommation humaine.
Infrastructures numériques		Points d'échange internet (IXP) Fournisseurs de services DNS Registres de noms de domaine de haut niveau.

D. Sanctions

Manquement	Sanction pénale (par manquement)	Sanction administrative (par manquement)
Défaut de notification d'un incident.	Emprisonnement de 8 jours à 1 an et amende pénale de 208 € (26 € x 8 (*)) à 160.000 € (20.000 € x 8 (*)) ou une de ces deux peines.	Amende administrative de 500 à 75.000 €
Non-respect de la confidentialité /du secret professionnel.	Emprisonnement d'un an à trois ans et amende pénale de 800 € (100 € x 8 (*)) à 8.000 € (1.000 € x 8 (*)) ou une de ces deux peines (voir art. 458 du Code pénal).	
Faire subir des conséquences négatives aux personnes ayant procédés de bonne foi à la notification d'un incident.		Amende administrative de 500 à 200.000 €
Récidive	En cas de récidive pour les mêmes faits dans un délai de trois ans, l'amende pénale est doublée et le contrevenant puni d'une peine d'emprisonnement de 15 jours à 3 ans.	En cas de récidive pour les mêmes faits dans un délai de trois ans, l'amende administrative est doublée.

(*) décimes additionnels applicables au mois d'avril 2020 – voir le site du SPF Justice pour une actualisation du coefficient multiplicateur des décimes additionnels.

E. Assistance technique

Le CCB assure, dans la mesure du possible, un support technique de première ligne pour les utilisateurs de la plate-forme.

L'équipe technique du CCB peut être contactée :

- par e-mail : cert@cert.be
- par téléphone : +32 (0)2 501 05 60

L'IBPT assure, dans la mesure du possible, un support technique de deuxième ligne pour les utilisateurs de la plate-forme.

L'équipe technique de l'IBPT peut être contactée :

- par e-mail : netsec@bipt.be
- par téléphone : +32 (0)2 226 88 88

F. Points de contact NIS

CENTRE POUR LA CYBERSECURITE BELGIQUE (CCB)
Rue de la Loi, 16
1000 Bruxelles

NIS Team	nis@ccb.belgium.be	+32 (0)2 501 02 11	www.ccb.belgium.be
CERT.be Team	cert@cert.be	+32 (0)2 501 05 60	www.cert.be

SERVICE PUBLIC FÉDÉRAL (SPF) INTÉRIEUR
CENTRE DE CRISE NATIONAL (NCCN)
Rue Ducale, 53
1000 Bruxelles

www.centredecrise.be/fr/contact

INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS
Département Sécurité réseau
Ellipse Building, Bâtiment C
Boulevard du Roi Albert II, 35
1030 Bruxelles

netsec@bipt.be
+ 32(0)2 226 88 88

www.bipt.be

SERVICE PUBLIC FEDERAL (SPF) ECONOMIE, P.M.E., CLASSES MOYENNES ET ENERGIE
DIRECTION GENERALE ENERGIE
Application énergie nucléaire et infrastructures critiques
Bd du Roi Albert II, 16
1000 Brussels

info.eco@economie.fgov.be (contact center)
+32 0800 120 33 (contact center)

www.economie.fgov.be/fr/nous-contacter

SERVICE PUBLIC FEDERAL (SPF) MOBILITE ET TRANSPORTS
CELLULE DE CRISE
City Atrium
Rue du Progrès, 56
1210 Bruxelles

info@mobilit.fgov.be
+32 (0)2 277 31 11

www.mobilit.belgium.be

LE SERVICE PUBLIC FEDERAL (SPF) SANTE PUBLIQUE,
SECURITE DE LA CHAINE ALIMENTAIRE
ET ENVIRONNEMENT
DIRECTION GENERALE SOINS DE SANTE
Eurostation II
Place Victor Horta, 40 bte 10
1060 Bruxelles

+32 (0)2 524.97.97

www.health.belgium.be

BANQUE NATIONALE DE BELGIQUE (BNB)
ORM – BCM Team
Boulevard de Berlaimont, 14
1000 Bruxelles

orm@nbb.be
+32 (0)2 221 21 11

www.nbb.be

AUTORITÉ DES SERVICES ET MARCHÉS FINANCIERS (FSMA)
Rue du Congrès, 12-14
1000 Bruxelles

+ 32(0)2 220 52 11

www.fsma.be

G. Références légales

- Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (*M.B.*, 3 mai 2019, p. 42857 et s) – « loi NIS ».

- Arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (*M.B.*, 18 juillet 2019, p. 72187 et s) – « AR NIS ».

- Règlement UE 2016/679 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 (Règlement générale sur la protection des données « RGPD »).

- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B., 5 septembre 2018, p. 68616 et s.).

- Article 36/47 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique (M.B., 28 mars 1998, p. 9377 et s).

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE SUR LES NOTIFICATIONS D'INCIDENTS NIS - OPÉRATEURS DE SERVICES ESSENTIELS (OSE)

Ce document et ses annexes ont été élaborés par le Centre pour la Cybersécurité Belgique (CCB), administration fédérale créée par l'arrêté royal du 10 octobre 2014 et sous l'autorité du Premier Ministre.

Tous les textes, mises en page, conceptions et autres éléments de toute nature dans ce document sont soumis à la législation sur les droits d'auteurs. La reproduction d'extraits de ce document est autorisé à des fins non commerciales exclusivement et moyennant mention de la source.

Le CCB décline toute responsabilité éventuelle en lien avec le contenu de ce document.

Les informations fournies :
• sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières ;
• ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points.

Éd. Responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles

Dépôt légal :
D/2020/14828/008

2020