Autorité de protection des données
Gegevensbeschermingsautoriteit

Autorisation (délivrée) n° 003/2026 du 5 octobre 2026

Objet: demande d'autorisation visée à l'article 21, § 4, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique : « Command-and-Control » (C2) – alertes - 4 (AUT-2026-00154)

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après, « l'Autorité »),

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données,* (ci-après, la « LCA ») ;

Vu l'article 21, § 4, de la loi du 26 avril 2024 *établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique* (ci-après, la « Loi NIS2 ») ;

Vu la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après, la « LCE ») ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil 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* (ci-après, le « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après, la « LTD »);

Vu les articles 44, 54 et 55 du Règlement d'Ordre Intérieur de l'Autorité de Protection des Données (ci-après, le « ROI ») ;

Vu la demande d'autorisation du Directeur Général du Centre pour la Cybersécurité Belgique, Monsieur Miguel De Bruycker (ci-après, « le Demandeur »), reçue le 16 septembre 2026 ;

Vu l'Autorisation de l'Autorité n° 001/2025 du 18 juillet 2025 *concernant une demande d'autorisation visée à l'article 21, § 4, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique: « Command-and-Control servers communicatiemetadata — waarschuwing » (AH-2025-0034)* (ci-après, « l'Autorisation n° 001/2025 ») ;

Vu l'Autorisation de l'Autorité n° 001/2026 du 16 février 2025 *concernant une demande d'autorisation visée à l'article 21, § 4, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique : « Command-and-Control » (C2) - alertes – 2 (AH-2025-0072)* (ci-après, « l'Autorisation n° 001/2026 ») ;

Vu l'Autorisation de l'Autorité n° 002/2026 du 25 juin 2026 *concernant une demande d'autorisation visée à l'article 21, § 4, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique : « Command-and-Control » (C2) - alertes – 3 (AUT-2026-00049)* (ci-après, « l'Autorisation n° 002/2026 ») ;

Vu la demande d'informations complémentaires adressée au Centre pour la Cybersécurité Belgique, le 23 septembre 2026 ;

Vu les informations complémentaires communiquées par le Centre pour la Cybersécurité Belgique, le 28 septembre 2026 ;

Vu la confirmation de la complétude du dossier envoyée au demandeur le 28 septembre 2026 ;

Prend, le 5 octobre 2026, la décision suivante :

I. Objet et contexte de la demande d'autorisation

1. Le Demandeur a introduit auprès de l'Autorité une Demande d'autorisation visée à l'article 21, § 4, de la Loi NIS2 (ci-après, « **la Demande** »). Cette Demande s'inscrit dans le cadre **des Autorisations n° 001/2025, n° 001/2026 et n° 002/2026** (ensemble, « **les Autorisations précédentes** »). L'Autorité renvoie par conséquent à ces Autorisations précédentes aux fins d'introduction et de contextualisation de la présente Demande. Elle s'y réfère également quant à la description du projet mis en œuvre dans ce contexte par le Demandeur (ci-après, « **le Projet** »). **La présente Autorisation doit être lue avec les Autorisations précédentes qui ensemble forment un tout**.

2. Le Demandeur a joint à sa Demande (catégorisée « SENSIBLE NON-CLASSIFIE (AR 20.12.2024) », « TLP :AMBER+STRICT ») les **deux annexes** (ensemble, « **la Documentation** ») suivantes, auxquelles il sera renvoyé comme indiqué ci-après :
   - « [redacted] », ci-après la « **Liste de C2S** », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT » ;
   - « [redacted] », ci-après la « **Note contextuelle** », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT ».

II. Examen

La présente décision est structurée comme suit et comporte une annexe :

II.1. Analyse 3
II.1.2. Approche suivie dans la présente Autorisation 3
II.1.2. Considérations relatives à la Demande 4
II.1.2.1. Eléments et sources sur la base desquels les adresses IP sont retenues 4
II.2.2.2. Lien entre les acteurs de la menace et la menace concernée 10
II.2.2.3. Justification des dates first seen 11
II.2.2.4. Mention des fondements légaux dans la Note contextuelle 13
II.2.2.4. Absence d'autre commentaire 14
II.2. Décision 14
[redacted] 21

II.1. Analyse

II.1.2. Approche suivie dans la présente Autorisation

3. Via la Demande, sont en substance demandés : l'accès à des métadonnées de communications électroniques relatives à **15 nouvelles adresses IP** et l'autorisation nécessaire à cet accès. La Demande du CCB (CSIRT National) s'inscrit strictement dans les limites juridiques et techniques des Autorisations précédentes de l'Autorité. Notamment, la Demande s'inscrit dans la même finalité et le même Projet, concerne les opérateurs Proximus, Telenet et Belnet et les mêmes métadonnées de communications électroniques. Le CCB (CSIRT National) confirme également que son Projet a été adapté conformément à l'Autorisation n° 002/2026 : « *S'agissant d'une demande subséquente à vos autorisations précédentes, il est renvoyé, pour toutes les informations complémentaires, aux éléments déjà fournis précédemment par le CCB.* ***Les modifications nécessaires ont été apportées aux***

procédures internes du CCB pour s'aligner entièrement aux éléments soulevés par l'APD dans son autorisation n° 002/2026 » (mis en gras par l'Autorité).

4. Autrement dit, **la présente Demande <u>ne soulève aucun nouveau questionnement de nature juridique ou technique</u>**, de telle sorte que l'Autorité se limite à renvoyer à ses Autorisations précédentes quant aux cadres normatif et technique du Projet, et en particulier quant à la base légale permettant au CCB (CSIRT National) de demander auprès des opérateurs des métadonnées de communication relatives au trafic ou à la localisation, et quant à l'exercice de sa mission par celui-ci justifiant de la nécessité et du caractère proportionné des demandes.

5. Avant tout, l'Autorité **observe et met en évidence le fait que le CCB (CSIRT National) a renforcé utilement le niveau de détail de la documentation communiquée à l'Autorité à l'appui de sa Demande** (la Note contextuelle et la Liste de C2S). Ce qu'elle accueille très favorablement. Ceci contribue à permettre un traitement plus efficace et rapide des demandes introduites, dans le délai légal particulièrement contraignant auquel est soumis l'Autorité.

6. Dans le cadre de la présente Demande, l'Autorité **s'est limitée à vérifier si dans les faits, sur la base des informations communiquées par le Demandeur** (à ce sujet, voir les considérants nos 90-93 de l'Autorisation n° 001/2025 et les considérant nos 23-39 et 42 de l'Autorisation n° 002/2026), **les adresses IP concernées relevaient bien du champ d'application de son Projet** et pouvaient par conséquent donner lieu à la collecte de métadonnées de communications électroniques auprès des opérateurs concernés, y compris concernant des communications passées pour lesquelles les opérateurs ont légalement conservé ces métadonnées (voir à ce sujet les considérants nos 19-28 de l'Autorisation n° 001/2026 ; considérants nos 23-39 et 46-50 de l'Autorisation n° 002/2026). A défaut, la collecte de métadonnées de communications électroniques auprès des opérateurs concernés serait contraire au RGPD (articles 5, 1., a), b) et c), et 6, 1., e)) et à la Loi NIS2 (article 21, § 2) et ne pourrait par conséquent pas être autorisée par l'Autorité.

7. **Ces vérifications ont mené aux commentaires suivants**.

<u>II.1.2. Considérations relatives à la Demande</u>

II.1.2.1. Eléments et sources sur la base desquels les adresses IP sont retenues

8. S'agissant des **<u>éléments et sources</u> sur la base desquels les adresses IP sont retenues** dans le cadre de la Demande, l'Autorité a interrogé le CCB (CSIRT National) concernant quatre adresses IP[1] à propos desquelles celui-ci a communiqué les informations complémentaires suivantes :

[redacted]

9. L'Autorité prend acte de ces réponses qui suffisent à étayer la Demande. L'Autorité souligne que les **informations de ce type devraient à l'avenir directement être intégrées dans la Note contextuelle** et rappelle qu'au plus la justification concrète avancée pour retenir une adresse IP est détaillée, au moins il y a de chances que l'Autorité soit amenée à poser une question additionnelle. Dans le contexte de [redacted], et dans les cas où une adresse IP est retenue sur la base d'un rapport produit par [redacted], il est toujours souhaitable que l'Autorité puisse disposer d'un résumé dudit rapport.

10. En réaction à une série de remarques adressées au CCB (CSIRT National) en la matière et reprises ci-après, celui-ci a également communiqué les informations complémentaires entre guillemets suivantes :

[1] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11. L'Autorité prend acte de ces informations complémentaires. Dans son Autorisation n° 002/2026 (point n° 14 du dispositif) l'Autorité a souligné que chaque demande d'autorisation dans le cadre du Projet, ainsi que chaque demande de contrôle ultérieur en cas d'urgence, devait continuer d'être accompagnée d'une note contextuelle détaillée selon les adresses IP concernées et les acteurs/moyens de la menace concernés, structurée de la même manière que la note contextuelle alors communiquée. **L'Autorité accueille très favorablement les améliorations et le renforcement apportés par le CCB (CSIRT National) à la Note contextuelle communiquée avec la Demande** : il convient de **continuer de procéder de cette manière** dans le cadre des demandes d'autorisation et de contrôles ultérieurs.

12. Cela étant précisé, **l'Autorité attire l'attention du CCB (CSIRT National) sur les points suivants qu'il convient de prendre en compte dans le cadre des demandes ultérieures** :

- Dès son Autorisation n° 001/2025 (considérant n° 61) l'Autorité a indiqué que le CCB (CSIRT National devait évaluer et indiquer le niveau de fiabilité des sources d'information, services et prestataires de services auxquels il recourt dans le cadre de la mise en œuvre du Projet. Dans ce contexte, l'Autorité attend que **l'ensemble** de ces sources, services et prestataires soient **précisément identifiés dans la Note contextuelle**. A cette fin, une description très succincte de ceux-ci peut être réalisée, pour autant que la Note contextuelle soit exhaustive et permette de retrouver aisément les informations détaillées pertinentes via internet (par exemple, en indiquant l'hyperlien vers le site officiel du prestataire concerné comme le CCB (CSIRT National) l'a mentionné dans les informations complémentaires communiquées à l'Autorité. **Étant entendu en outre que la Note contextuelle doit être dépourvue d'ambiguïté concernant la fiabilité de la source concernée** ;

- S'agissant du recours à [redacted] **et à la prise en compte des** [redacted] **premièrement,** l'Autorité souligne que **lorsqu**[redacted] **n'est plus associé** [redacted] **depuis un certain temps, la valeur probante** [redacted] **commence à perdre de son intérêt**. [redacted] **Il est donc important que le CCB précise,** [redacted] **à quelle date** [redacted] **a pris fin et pourquoi le CCB considère encore** [redacted] **pertinentes.**

  Deuxièmement, il convient **d'indiquer systématiquement la date à laquelle** [redacted] est utilisé dans le cadre de l'analyse menée par le CCB (CSIRT National).

  Troisièmement enfin, les résultats obtenus via le service de [redacted] sont particulièrement pertinents si [redacted]. Mais **l'Autorité doit pouvoir comprendre les résultats retenus selon la finalité poursuivie** [redacted]. A cette fin, l'Autorité attend, dans les futures demandes, que le CCB (CSIRT National) indique avoir procédé à une vérification [redacted] et précise également

[redacted]

II.2.2.2. Lien entre les acteurs de la menace et la menace concernée

13. Concernant le **lien entre les acteurs de la menace et la menace concernée** (une menace grave contre la sécurité publique relevant de l'espionnage), l'Autorité a décidé ce qui suit au considérant n° 29 (et point 5., dernier tiret du dispositif) de son Autorisation n° 002/2026 :

> « *S'agissant de l'identification de menaces graves pour la sécurité publique, il importe que la Demande (en l'occurrence, la Note contextuelle)* ***lie concrètement chaque adresse IP à des faits susceptibles de constituer une menace grave pour la sécurité publique****. A cet égard, compte-tenu de la* ***finalité préventive*** *du Projet, la relation entre l'adresse IP concernée et une menace grave pour la sécurité publique peut être établie dans les hypothèses suivantes :*
>
> - *A supposer que l'adresse IP concernée puisse être liée, sur la base des éléments avancés dans la Demande, à un* ***acteur (ou moyen) de la menace****, la motivation (la Note contextuelle) doit lier l'acteur de la menace, au moins sur la base d'indices objectifs et sérieux, à de tels faits (par exemple en l'état, la Note contextuelle se réfère régulièrement à des rapports publics liant certains acteurs/moyens aux menaces décrites – espionnage par exemple – sans toutefois indiquer la référence de ces rapports[2]). L'Autorité insiste sur l'importance (au-delà de l'identification précise de la source d'information sur la base de laquelle le CCB (CSIRT National) a identifié l'adresse IP concernée, ci-après),* ***de décrire concrètement l'acteur de la menace et d'illustrer les actions déjà entreprises par celui-ci sur la base de sources fiables****, ou selon le cas,* ***de décrire le moyen de la menace*** [redacted] ***) et la manière dont il a déjà été utilisé par divers acteurs de la menace sur la base de sources fiables.*** *L'Autorité comprends que selon les cas, les moyens/l'infrastructure sont susceptibles d'être développés et opérés par les acteurs concernés, de telle sorte qu'il peut être référé aux deux via un même nom ;* ***et/ou***
>
> - *Il existe des indices sérieux (par exemple, la source utilisée par le CCB (CSIRT National) pour retenir l'adresse IP concernée) sur la base desquels* ***l'adresse IP concernée*** *a été utilisée en relation avec de tels faits (par exemple : l'adresse IP donne accès à une*

---

[2] « [redacted]

[3] [redacted]

[4] [redacted]

infrastructure illégale dédiée à l'espionnage ; l'adresse IP est retrouvée dans le code d'un malware comme cela a été le cas dans une des demandes d'autorisation antérieures ; etc.) » (numérotation des notes de bas de page modifiée dans la présente Autorisation).

14. Dans la Note contextuelle, certains acteurs sont très succinctement décrits et surtout, ils ne semblent pas encore connus sur la base des informations disponibles via une recherche sommaire dans les ressources publiquement accessibles via Internet. Il en est ainsi de [redacted]. L'Autorité a interrogé le Demandeur à ce sujet[5] et celui-ci a communiqué les informations complémentaires suivantes :

[redacted] (mis en gras par l'Autorité).

15. L'Autorité prend acte de ces explications et **relève qu'effectivement, dans la Note contextuelle,** bien que ces acteurs de la menace soient insuffisamment mis en relation factuelle avec [redacted] dans leur description, **les adresses IP liées aux acteurs concernés sont quant à elles bien liées à des moyens relatifs à** [redacted]

II.2.2.3. Justification des dates first seen

16. A propos des **dates *first seen***, l'Autorité a décidé, aux considérant nos 25 et 28 de l'Autorisation n° 001/2026 (voir encore le point n° 5., avant-dernier tiret, du dispositif de l'Autorisation n° 002/2026) que **chaque date *first seen* retenue devait être associée, dans la documentation conservée par le Demandeur, à un événement concret indiquant un lien entre l'activité**

[5] [redacted]

concernée du serveur C2 visé par la Demande et l'adresse IP concernée. Ceci est déterminant dès lors que l'événement concerné justifie la raison pour laquelle les métadonnées de communications électroniques **passées** sont recherchées.

17. Or à ce sujet, dans la Note contextuelle, en ce qui concerne les dates *first seen* différentes de la date de la Demande, celles-ci **ne sont pas directement justifiées en tant que telles, en relation avec des événements concrets pertinents** ([redacted]) et ne semblent généralement pas non plus indirectement reliables à de tels événement sur la base des informations transmises. Ce dernier point est à l'exception de deux des adresses IP que l'Autorité pourrait relier à des événements précis [redacted] Étant entendu dans ces deux cas que la date concernée correspond à la date de la Demande du CCB (CSIRT National) – soit le 14 septembre 2026. **L'Autorité présume que les dates *first seen* sont probablement liées aux [redacted] identifiés dans la Note contextuelle**. **Cela étant précisé, à défaut pour ceux-ci d'être datés, l'Autorité ne peut le vérifier**. Remarque : l'Autorité a fait part de ce constat au Demandeur qui a précisé ce qui suit : « *Pour l'ensemble des adresses IP liées à [redacted] la date « first seen » correspond à la première fois que les adresses IP ont été scannées sur [redacted] Pour les autres, la date first seen correspond à la date à laquelle l'adresse a été validée pour la première fois [redacted]* […] ».

18. S'agissant de l'accès à des métadonnées de communications électroniques **passées** (plus précisément, des communications électroniques qui ont eu lieu avant la date de décision du CCB (CSIRT National) d'introduire sa Demande[6]), **le CCB (CSIRT National) doit adapter sa documentation** de manière telle que les dates *first seen* soient directement associées à un événement concret indiquant un lien entre l'activité concernée du serveur C2 visé par la Demande et l'adresse IP concernée. ***Le cas échéant*, les dates *first seen* devront être adaptées.** D'un point de vue formel, cet événement ne doit pas nécessairement être répété à côté de la date *first seen* elle-même (bien que cette solution ait le mérite de la plus grande clarté). Mais il **doit être daté et aisément et directement identifiable en tant que tel par l'Autorité**, en particulier compte-tenu du fait qu'il ne soit pas exclu à l'avenir que la fréquence des Demandes augmente et que celles-ci concernent de plus nombreuses adresses IP. Le CCB (CSIRT National) est **libre quant à la forme retenue**.

19. Pour le reste, au considérant n° 34 de son Autorisation n° 001/2025, lorsque le CCB (CSIRT National) n'envisageait que les collectes de métadonnées de communications électroniques qui allaient se

[6] Voir le considérant n° 19 pour ce qui concerne les métadonnées de communications électroniques à collecter à partir de la date de la Demande du CCB (CSIRT National).

produire à compter de la date à laquelle la demande du CCB (CSIRT National) serait adressée aux opérateurs (c'est-à-dire, des communications futures), l'Autorité avait déjà mis en évidence que dans le cadre du Projet, le Demandeur pourrait également demander l'autorisation de traiter les métadonnées relatives aux communications électroniques émises à partir de la date d'introduction de sa demande d'autorisation auprès de l'Autorité. Dans un tel scénario, où la date *first seen* correspond en fait à la date de la Demande introduite par le CCB (CSIRT National), il suffit que la documentation produite renseigne des événements concrets pertinents datés au plus tard au jour auquel le CCB (CSIRT National) décide de retenir l'adresse IP concernée dans la Demande qu'il va adresser à l'Autorité. A cet égard, il se peut qu'il existe une différence de quelques jours entre le moment où le CCB (CSIRT National) décide de la demande à adresser à l'Autorité et la date de réception de celle-ci par l'Autorité, ce qui est indifférent sur le plan des principes. **Ce qui importe est que l'Autorité puisse être en mesure de constater, dans cette situation, que la date *first seen* retenue est la date de la Demande du CCB (CSIRT National)**.

20. Enfin, l'Autorité observe une **discordance dans la documentation communiquée concernant l'adresse** [redacted]: il existe une différence d'année dans la date retenue selon qu'il s'agisse de la Note contextuelle ([redacted]) ou de la Liste de C2S ([redacted]). L'Autorité comprend qu'il convient de retenir la date [redacted] – ce que le Demandeur a confirmé. De nouveau cependant, **cette date n'est directement liée à aucun événement concret** [redacted] **La documentation du CCB (CSIRT National) <u>doit être adaptée</u> sur ce point et *le cas échéant*, la date *first seen* retenue doit également être adaptée**.

II.2.2.4. Mention des fondements légaux dans la Note contextuelle

21. En ce qui concerne les **<u>fondements légaux</u>** de la conservation des métadonnées par les opérateurs concernés et de l'accès par le CCB (CSIRT National) à ces données, la Note contextuelle indique ce qui suit :

> « *Legal basis :*
> *- Retention by ISP: artikelen 122, § 4/1; en 126/1, § 1 en § 2 WEC*
> *- Access by CCB: artikelen 127/1, § 2, 2°, 4° en 6°, en § 4 WEC* ».

22. En l'occurrence, la Demande s'inscrit dans le cadre de **la prévention d'une menace grave contre la sécurité publique**. Le CCB (CSIRT National) indique à ce propos dans sa Demande que « *En ce qui concerne les liens entre les adresses IP fournies, les malwares, les groups malicieux et la menace grave pour la sécurité publique, nous nous permettons de renvoyer vers les considérations émises par*

le CCB dans le cadre de l'autorisation n° 002/2026 ». Les 15 adresses IP concernées relèvent de la menace d'espionnage. Ce sont par conséquent les articles 127/1, § 2, **2°**, de la LCE et 21, § 2, 2°, de la Loi NIS2 qui sont applicables s'agissant des données conservées en exécution des articles **126/1 à 126/3 de la LCE**. **La référence aux fondements légaux applicables dans la Note contextuelle doit être adaptée** à cet égard dès lors que l'application de l'article 127/1, § 2, **6°** (prévention de la criminalité grave) n'est pas sollicitée (se référer à ce sujet à l'Autorisation n° 002/2026).

23. Par ailleurs, si le CCB (CSIRT National) peut, **selon la finalité poursuivie**, prétendre accéder aux métadonnées conservées sur la base des **articles 122 et 123 de la LCE** à la fois en tant qu'autorité compétente aux fins de la prévention de menaces graves pour la sécurité publique visée à l'article 127/1, § 2, **2°**, de la LCE, et en tant qu'autorité compétente pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information visée à l'article 127/1, § 2, **4°**, de la LCE, conformément à l'article 127/1, § 4, al. 1er, de la LCE, le CCB (CSIRT National) n'est pas autorisé à accéder aux métadonnées conservées sur la base des articles 126/1 et 126/3 de la LCE en tant qu'autorité compétente pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information. **La Note contextuelle doit être clarifiée sur ce point en distinguant les fondements légaux appliqués**.

II.2.2.4. Absence d'autre commentaire

24. Les vérifications menées par l'Autorité n'appellent pas d'autre commentaire.

II.2. Décision

L'Autorité, dans les limites rappelées aux considérants nos 12-17 de l'Autorisation n° 001/2025 et aux considérants nos 6-7 de l'Autorisation n° 001/2026, en prenant acte que les modifications nécessaires ont été apportées aux procédures internes du CCB (CSIRT National) pour se conformer entièrement aux éléments soulevés dans l'Autorisation n° 001/2026 (considérant n° 3 de l'Autorisation n° 002/2026) et aux éléments soulevés dans l'Autorisation n° 002/2026 (**considérant n° 3**) décide que

> **1.** Le Demandeur doit indiquer clairement à l'Autorité, dans les 10 jours ouvrables à compter de la communication de la présente décision (la date d'envoi du courrier électronique à l'attention du Demandeur, par l'Autorité, faisant foi), les passages de sa décision qui selon lui, ne peuvent pas être publiés aux motifs avancés par lui (considérants nos 6-11 de l'Autorisation n° 001/2025 ; considérants nos 2-4 de l'Autorisation n° 001/2026) ;

2. Chaque demande concrète d'autorisation d'accès à des métadonnées de communications électroniques auprès d'un opérateur doit être soumise pour autorisation préalable à l'Autorité. Ce qui n'exclut pas que les demandes d'autorisations subséquentes, ou de contrôle ultérieur en cas d'urgence, puissent se référer à la présente décision ainsi qu'à l'Autorisation n° 001/2025 et à l'Autorisation n° 001/2026, pour autant qu'elles restent motivées de manière circonstanciée pour le surplus.

L'Autorité est favorable à la démarche suivie par le Demandeur consistant à lui soumettre une demande d'autorisation préalable compte-tenu des modifications de son Projet, plutôt que, à supposer que l'urgence puisse être invoquée dans le cadre de sa Demande, de placer l'Autorité devant le fait accompli, dans une situation de contrôle ultérieur. Une telle approche garantit un travail plus efficace et plus sûr sur le plan juridique. Elle attend du Demandeur à l'avenir qu'il identifie clairement les considérants de ses décisions d'autorisation qui nécessiteraient des adaptations en raison de la modification du Projet (considérants nos 18-24 de l'Autorisation n° 001/2025 ; considérants nos 6-7 de l'Autorisation n° 001/2026) ;

3. Le Projet est fondé sur l'article 19, § 1er, 2°, de la Loi NIS2. Il s'agit de diffuser des messages d'alerte et des informations sur les cybermenaces et les vulnérabilités auprès des entités et personnes potentiellement victimes concernées, après avoir réalisé les actes d'analyse et de détection nécessaires à cette fin (considérants nos 25-29 de l'Autorisation n° 001/2025 ; considérants nos 29-31 de l'Autorisation n° 001/2026) ;

4. Toute demande d'autorisation préalable doit indiquer le ou les opérateurs concernés par la demande d'autorisation (considérants nos 33-36 de l'Autorisation n° 001/2025) ;

5. Les métadonnées relatives à des communications électroniques antérieures à la date de la présente décision ne peuvent être collectées sur la base des dates « first seen » identifiées par le CCB (CSIRT National) (se référer à la Note contextuelle et à la Liste de C2S) que si les quatre conditions suivantes sont remplies (considérants nos 19-28 de l'Autorisation n° 001/2026 ; considérants nos 23-29 et 46-50 de l'Autorisation n° 002/2026) :

- Les métadonnées sont collectées sur la base de fondements légaux précis (article et selon, paragraphe, alinéa, littera et numéro) explicitement et clairement identifiés par le CCB (CSIRT National) à l'attention des opérateurs ;

- Les métadonnées sont conservées légalement par les opérateurs concernés, conformément aux articles 122 et 123 ou 126/1 de la LCE, en fonction du fondement légal de la demande ;

- Le Demandeur met en place un processus permettant la prise en compte directe dans le cadre de son Projet, de l'arrêt attendu de la Cour de justice : il doit réévaluer la licéité des traitements de métadonnées mis en œuvre dans le cadre du Projet sur la base de ce dernier, et en tirer les conséquences ;

- Chaque date « *first seen* » retenue est associée, dans la documentation conservée par le Demandeur, à un événement concret indiquant un lien entre l'activité concernée du serveur C2 visé par la Demande et l'adresse IP concernée. Si cette date est trop ancienne au regard des délais de conservation licite des métadonnées par les opérateurs, la date des métadonnées qui peuvent être collectées devra être adaptée en conséquence dans la documentation du Demandeur.

  La Note contextuelle doit être adaptée sur ce point et les dates *first seen* doivent le cas échéant être modifiées (**considérants nos 16-20**) ;

- Lorsque sont concernées des données conservées conformément à l'article 126/1 de la LCE, pour chaque adresse IP concernée, le demandeur doit indiquer dans sa demande, selon le fondement légal sollicité, la menace grave pour la sécurité publique qui est concernée (articles 126/1, § 1er, al. 3, et 127/1, 2°, de la LCE, et article 21, § 2, 2°, de la Loi NIS2) ou le fait relevant de la criminalité grave concerné (articles 126/1, § 1er, al. 3, et 127/1, 6°, de la LCE, et article 21, § 2, 1°, de la Loi NIS2), et la relation entre ceux-ci et l'adresse IP concernée. Dans ce contexte, une attention particulière doit être réservée à la description de l'acteur (ou du moyen) de la cybermenace concernée ;

  Dans le cadre de la présente Demande, les [redacted] adresses IP concernées concernant une menace grave pour la sécurité publique en relation avec [redacted], les articles 126/1, § 1er, al. 3, et 127/1, 2°, de la LCE, et article 21, § 2, 2°, de la Loi NIS2 sont applicables. La Note contextuelle doit être adaptée en ce sens (**considérants nos 5-23**).

6. Le Projet peut concerner les métadonnées de communications électroniques entre les C2-servers et les entités essentielles ou importantes visées par la Loi NIS2, ainsi que les métadonnées de communications électroniques entre ces C2-servers et d'autres entités, y compris des personnes physiques (considérants nos 37-44 de l'Autorisation n° 001/2025). L'Autorité prend acte des démarches qui ont été entreprises par le Demandeur ainsi que du

fait qu'une disposition interprétative ait été adoptée concernant la Loi NIS2. La préoccupation exprimée par l'Autorité dans son Autorisation n° 001/2025 portait sur le fait que le Projet puisse impliquer un certain monitoring en temps réel au niveau des opérateurs, du trafic IP d'entités qui ne sont pas des entités NIS2, à savoir et entre autres, des entités (y compris des personnes physiques) qui ne sont pas la première et principale cible, compte-tenu de leurs finalités, des dispositifs normatifs européen et belge NIS2 (considérants nos 69-73 de l'Autorisation n° 001/2026) ;

7. L'identification d'une victime se fait sur la base de plusieurs éléments : [redacted] (considérants nos 46-50 de l'Autorisation n° 001/2025) ;

8. La collecte auprès de sources d'identification des adresses IP listées par le demandeur dans le cadre du Projet doit être conforme à la Loi NIS2. En outre, le Projet nécessite la mise en place d'un processus efficace de vérification de la qualité des informations relatives aux C2-servers communiquées par l'ensemble de ces sources et partant, du fait que les adresses IP concernées sont effectivement dédiées au trafic de C2-servers sélectionnés sur la base de la gravité de l'impact de leurs activités. Ce processus doit comprendre les combinaisons pertinentes de mesures techniques communiquées par le Demandeur dans le cadre de l'Autorisation n° 001/2025 et de l'Autorisation n° 001/2026 (considérants nos 48-52 de l'Autorisation n° 001/2026), ainsi que le cas échéant, toute autre mesure supplémentaire qu'exigerait l'état de la technique en la matière. Enfin, le Demandeur doit évaluer et indiquer le niveau de fiabilité des sources d'informations, services et prestataires de services auxquels il recourt dans le cadre de la mise en œuvre du Projet. Ces processus et leur mise en œuvre doivent être documentés au titre de l'*accountability* (considérants nos 52-61 de l'Autorisation n° 001/2025).

L'Autorité prend acte de la bonne pratique mise en œuvre par le CCB (CSIRT National) consistant à faire analyser et vérifier par au moins deux analyses les informations communiquées par ses partenaires externes. Elle prend également acte du fait que [redacted]

(considérant n° 40 de l'Autorisation n° 002/2026) ;

9. Le Projet nécessite la mise en place d'un processus efficace de contrôle au moins hebdomadaire et plus fréquent si cela se justifie, de l'actualité de la pertinence de chaque

adresse IP concernée au regard du Projet (vérification que l'adresse reste dédiée aux activités d'un serveur C2), basé sur les mesures de vérification visées aux considérants nos 57 et 59 de l'Autorisation n° 001/2025 (voir également les considérants nos 40-42 de l'Autorisation n° 002/2026), à charge pour le CCB de conserver une trace, au titre de son obligation d'accountability, de la justification de la périodicité retenue à l'aune de la dynamique des activités du serveur C2 concerné, de l'état de la technique et des bonnes pratiques pertinentes (considérants nos 53-54 de l'Autorisation n° 001/2026) ;

10. Le Projet nécessite que, dès que le CCB (CSIRT National) constate qu'une adresse IP n'est plus liée au C2-server concerné, l'opérateur concerné en soit immédiatement notifié via un canal adapté et cesse dès ce moment la collecte des métadonnées relatives au trafic depuis et vers l'adresse concernée. Le Projet doit également prévoir un processus aussi efficace de notification à l'attention du CCB (CSIRT National) cette fois, lorsque l'opérateur concerné dispose d'éléments objectifs de nature à questionner l'exactitude des données concernées. L'Autorité doit être informée des mises à jour opérées à l'égard de la liste de C2-servers dans ce contexte, à l'occasion de la prochaine demande d'autorisation (ou de contrôle ultérieur) qui lui est adressée dans le cadre du Projet (considérants nos 67-70 de l'Autorisation n° 001/2025) ;

11. Le CCB, dans les limites de ses possibilités et compétences, doit envisager la possible mise en œuvre simultanée par des tiers, de techniques de blocage/filtrage par les opérateurs concernés des adresses IP dédiées aux C2-servers concernés, de manière à prévenir la réalisation des menaces concernées. Etant entendu que c'est bien au CCB (CSIRT National) *in fine* et *in concreto*, qu'il appartient d'apprécier, dans l'exercice de sa mission légale et en utilisant la marge de manœuvre dont il jouit à cette fin, si et quand une mesure alternative de blocage/filtrage par un tiers pourrait être utile, afin de garantir le meilleur niveau de sécurité compte-tenu de la politique qu'il mène en la matière (considérants nos 38-44 de l'Autorisation n° 001/2026) ;

12. Compte-tenu de sa finalité, à l'aune des principes de finalité et de proportionnalité (y compris la minimisation des données), le Projet nécessite d'envisager la mise en œuvre simultanée, dans la mesure du possible (sur la base des informations à disposition du CCB (CSIRT National) et des risques pour la cybersécurité), d'une information générale (pas seulement à l'attention des victimes concernées) à propos des C2-servers et adresses IP concernés via « Cyber Threat Alerts » (considérants nos 79-81 de l'Autorisation n° 001/2025 ; considérants nos 45-47 de l'Autorisation n° 001/2026) ;

13. Le CCB (CSIRT National) doit à tout le moins indiquer dans les demandes adressées aux opérateurs, par adresse IP : le pays d'origine de l'adresse IP concernée ainsi que la menace/l'activité malveillante concrète (ransomware, espionnage, etc. ; soit, selon le fondement légal de sa demande, la menace grave pour la sécurité publique concernée ou le fait relevant de la criminalité grave concerné) concernée pour la Belgique (se référer sur ce point aux considérants nos 56 et 58 de l'Autorisation n° 001/2025) (considérants nos 55-61 de l'Autorisation n° 001/2026) ;

14. Chaque demande d'autorisation dans le cadre du Projet, ainsi que chaque demande de contrôle ultérieur en cas d'urgence, doit continuer d'être accompagnée d'une note contextuelle détaillée selon les adresses IP concernées et les acteurs/moyens de la menace concernés, structurée de la même manière que la Note contextuelle communiquée dans le cadre de la Demande adressée à l'Autorité dans le contexte de l'Autorisation n° 002/2026, le cas échéant précisée à l'aune des considérations développées dans les considérants nos 23-29 de l'autorisation n° 002/2026. [redacted] ; sans préjudice de la possibilité pour l'Autorité de demander à l'appui des demandes ultérieures la communication des documents sur la base desquels le CCB (CSIRT National) identifie les adresses IP dédiées aux C2-servers comme étant pertinentes dans le cadre du Projet (considérants nos 90-93 de l'Autorisation n° 001/2025 ; considérant n° 42 de l'Autorisation n° 002/2026).

L'Autorité accueille très favorablement les améliorations et le renforcement apportés par le CCB (CSIRT National) à la Note contextuelle communiquée avec la Demande, bien que certains points doivent encore retenir l'attention du CCB (CSIRT National) (**considérants n° 8 et nos 11-12**). L'Autorité souligne que, plus l'information contextuelle pertinente est détaillée, moins il y a de chance qu'elle s'interroge sur les éléments ayant conduit à la sélection de l'une ou l'autre adresse IP.

L'Autorité prend acte des précisions complémentaires communiquées par le CCB (CSIRT National) concernant les acteurs de la menaces identifiés [redacted] et leur relation avec des moyens de la menace [redacted] (**considérants nos 14-15**).

15. L'Autorité n'est pas compétente, au stade de sa saisine en vue de la délivrance d'une autorisation, pour se prononcer à propos de l'exercice par les personnes concernées, de leurs droits tels que prévus aux articles 12 à 21 du RGPD. Les considérations développées à ce sujet

dans l'Autorisation n° 001/2026 sont communiquées à titre purement indicatif (considérants nos 65-68 de l'Autorisation n° 001/2026) ;

16. Les métadonnées de communications électroniques collectées par le CCB (CSIRT National) ne peuvent pas être traitées ultérieurement en vue de l'accomplissement d'une autre finalité que celle visée par le Projet (considérants nos 103-110 de l'Autorisation n° 001/2025).

L'Autorité n'est toutefois pas compétente, au stade de sa saisine en vue de la délivrance d'une autorisation, pour se prononcer à propos des traitements ultérieurs de données fondés sur des obligations légales s'imposant au CCB (CSIRT National). Les considérations développées à ce sujet dans l'Autorisation n° 001/2026 sont communiquées à titre purement indicatif (considérants nos 32-37 de l'Autorisation n° 001/2026) ;

17. Les métadonnées collectées peuvent être conservées jusqu'à la fin de l'investigation et de l'avertissement des victimes, et jusqu'à maximum un an à partir de leur collecte initiale à des fins d'*accountability*. Elles peuvent également être conservées pendant cette durée afin de permettre la réalisation du traitement d'analyse de données identifié dans la réponse communiquée par le Demandeur (dans le cadre de l'Autorisation n° 001/2026) afin d'identifier des « [redacted] », « [redacted] ». Cela étant précisé, conformément au principe de minimisation des données, ces analyses doivent être réalisées sur la base de données anonymisées et à défaut, si cela s'avérait impossible en pratique (ce qui devrait être documenté conformément au principe d'*accountability*), sur la base de données agrégées (considérants nos 111-114 de l'Autorisation n° 001/2025 ; considérants nos 62-64 de l'Autorisation n° 001/2026) ;

18. Dans les conditions et limites visées ci-avant et dans la présente décision, conformément aux articles 122, 123, 127/1, § 2, 2°, et 126/1, § 1er, al. 3 de la LCE, et, et 21, §§ 2, 2°, et 4, de la Loi NIS2, le CCB agissant en tant que CSIRT National est autorisé à collecter auprès des opérateurs Belnet, Proximus et Telenet, les métadonnées de communications électroniques suivantes, *Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes*, relatives aux communications électroniques émises vers et depuis les 15 adresses IP dédiées à des C2-servers contextualisées dans la Note contextuelle (p. 1) et reprises dans l'Annexe 1 ci-après, à partir des dates « *first seen* » le cas échéant adaptées (considérants nos 15-20), et ce, aussi longtemps que les adresses IP concernées sont dédiées aux C2-servers concernés ;

19. La présente décision peut faire l'objet d'un recours devant le Conseil d'Etat.

Pour le Service d'Autorisation et d'Avis,
(sé) Alexandra Jaspar, Directrice