Autorité de protection des données
Gegevensbeschermingsautoriteit

**Autorisation (délivrée) n° 002/2026 du 25 juin 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 - 3** (AUT-2026-00049)

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 8 mai 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 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 – 2 (AH-2025-0072)* (ci-après, « l'Autorisation n° 001/2026 ») ;

Vu la demande d'informations complémentaires adressée au Centre pour la Cybersécurité Belgique, le 21 mai 2026 ;

Vu les informations complémentaires communiquées par le Centre pour la Cybersécurité Belgique, le 12 juin 2026 ;

Vu la confirmation de la complétude du dossier envoyée au demandeur le 12 juin 2026 ;

Prend, le 25 juin 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 est en relation directe avec **l'Autorisation n° 001/2025** et **l'Autorisation n° 001/2026** (ensemble, « **les Autorisations précédentes** ») **dans le cadre desquelles elle s'inscrit**. L'Autorité renvoie à ses 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** » du Demandeur). **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 ».

3. Dans sa Demande, le CCB (CSIRT National) indique qu'il « *entend obtenir une nouvelle autorisation préalable, pour une nouvelle liste d'adresses IP dans le cadre des conditions formulées à l'occasion des autorisations n°001/2025 et n°001/2026* ». Il précise encore que « *S'agissant d'une demande subséquente* [aux] *autorisations n°001/2025 et n°001/2026, 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 001/2026*** » (mis en gras par l'Autorité). L'Autorité en prend acte.

4. Via la Demande, sont en substance demandés : l'accès à de nouvelles métadonnées de communications électroniques et l'autorisation nécessaire à cet accès moyennant l'extension du fondement légal sollicité.

## II. Examen

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



### II.1. Fondements légaux de la conservation et de l'accès aux métadonnées concernées

5. L'Autorité observe que la Demande introduite par le Demandeur, en son considérant n° 6, vise les métadonnées « *conservées conformément aux délais visés aux articles 122* ***et suivants*** *de la LCE* » (mis en gras par l'Autorité), et que la Note contextuelle se réfère systématiquement, quant à la

« *Retention by ISP* », à l'article 126/1, §§ 1 et 2 de la LCE, et quant à l' « *Access by CCB* », à l'article 127/1, § 2, 2°, 4° et 6°, et § 4, de la LCE.

6. L'article **126/1** de la LCE prévoit notamment ce qui suit :

> « *Art. 126/1.[1 § 1er. Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, conservent les données visées à l'article 126/2, § 2,* ***pour les zones géographiques visées à l'article 126/3, pendant douze mois à partir de la date de la communication,*** *sauf si une autre durée est fixée dans l'article 126/3.*
>
> *Chaque opérateur conserve les données qu'il a générées ou traitées dans le cadre de la fourniture des services et réseaux de communications électroniques concernés.*
>
> *Ces données* ***sont conservées aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique,*** *et de la sauvegarde des intérêts vitaux d'une personne physique.*
>
> *§ 2. Les métadonnées de communications électroniques, en ce compris les métadonnées pour les appels infructueux, auxquelles s'applique l'obligation de conservation visée au paragraphe 1er, sont énumérées à l'article 126/2, § 2.*
>
> *§ 3. Les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée à l'article 126/3 ou vers une telle zone.*
>
> […] » (mis en gras par l'Autorité).

7. L'article **127/1** de la LCE prévoit notamment ce qui suit :

> « *Art. 127/1.*
>
> […]
>
> *§ 2. Seules les autorités suivantes peuvent obtenir d'un opérateur des données conservées en vertu des articles 122 et 123, pour les finalités ci-dessous, pour autant que prévu par et aux conditions fixées dans une norme législative formelle:*
>
> *1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;*
>
> ***2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique****;*

*3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques;*

***4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information;***

*5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques;*

***6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave**;*

*7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;*

*8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave;*

*9° l'Institut dans le cadre du contrôle de la présente loi et les autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle;*

*10° les autorités qui sont légalement habilitées à réutiliser des données à des fins de recherche scientifique ou historique ou à des fins statistiques.*

*§ 3. Les données conservées en vertu des articles 126 et 127 le sont pour les autorités et les finalités visées au paragraphe 2, 1° à 8°.*

[...]

*§ 4. Les données conservées en vertu des articles **126/1** et 126/3 le sont **pour les autorités et finalités visées au paragraphe 2, 1° à 3° et 6°.***

*Seules les autorités visées au paragraphe 2, 1° à 3°, 6° et 9°, peuvent obtenir d'un opérateur, pour les finalités visées dans ce même paragraphe, des données conservées en vertu des articles 126/1 et 126/3, pour autant que prévu par et aux conditions fixées dans une norme législative formelle.*

*§ 5. La norme législative formelle de droit belge visée aux paragraphes 2 à 4 précise:*

*- la ou les catégories d'entreprises auxquelles l'autorité peut demander des données;*

*- les catégories de données qui peuvent être demandées;*

*- les finalités poursuivies;*

*- les mécanismes de contrôle de la demande de données, qui est effectué en interne ou, le cas échéant, par une juridiction ou une autorité administrative indépendante.*

*Le ministre fait publier au Moniteur belge une circulaire qui comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127.*

*A la demande du ministre ou de l'Institut, les autorités belges visées aux paragraphes 2 à 4 fournissent les informations nécessaires pour la rédaction de cette circulaire.*

[…] » (mis en gras par l'Autorité).

8. Cependant, la Demande adressée à l'Autorité dans le cadre de l'Autorisation **n° 001/2026**, qui étendait l'accès aux métadonnées initialement envisagé par le CCB (CSIRT National) aux métadonnées relatives à des communications électroniques ayant eu lieu dans le passé[1], visait, en son paragraphe n° 6, les métadonnées « *conservées conformément aux délais **visés aux articles 122 et 123 de la LCE*** » (mis en gras par l'Autorité).

9. **Or ces deux hypothèses de conservation des données sont différentes.** Dans le cadre des articles **122 et 123**, il s'agit en principe (sous réserves des obligations fixées par le droit belge et des questionnements pendants devant la Cour de justice en la matière) d'accéder à des métadonnées qui sont conservées par les opérateurs **pour leurs propres finalités**. Tandis que l'article **126/1** de la LCE vise une hypothèse dans laquelle ceux-ci sont **obligés** de conserver des métadonnées de communications électroniques pour les **finalités poursuivies par des autorités publiques**. Cette ingérence plus importante dans les droits et libertés des personnes concernées est permise « *aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique* », afin de contribuer à l'exercice par les autorités publiques compétentes concernées de leurs propres missions.

**II.2. Articles 126/1 et 127/1 de la LCE : cadre juridique**

10. **La sollicitation complémentaire de l'article 127/1, § 2, 2° et 6°, en combinaison avec les finalités poursuivies à l'article 21, § 2, 1° et 2°, de la Loi NIS2, dans le cadre des tâches visées à l'article 19, § 1er, 2°, de la Loi NIS2** (diffusion de messages d'alertes, soit la finalité du Projet), **nécessite une motivation spécifique**, toujours en relation avec la Belgique (finalité du Projet). Il s'agit dans ce cadre de justifier de « *menaces graves pour la sécurité publique* » et/ou de « *fait*[s] *qui relève*[nt] *de la criminalité grave* » telle que définie par la LCE, et ce, dans les limites fixées dans la jurisprudence de la Cour de justice.

[1] La demande adressée à l'Autorité dans le cadre de l'Autorisation n° 001/2025 ne visait que les métadonnées relatives à des communications électroniques ayant lieu à partir de la délivrance par l'Autorité de son autorisation.

11. A cet égard, il se dégage de la Note contextuelle que les menaces concernées semblent concerner [redacted] relèverait plutôt de la sécurité nationale (concept qui reste distingué du concept de sécurité publique, tant par la Loi NIS2 que par la Directive elle-même). Et la Documentation communiquée ne vise pas les dispositions du Code pénal qui seraient concernées (infractions relevant de la criminalité grave, commises en ligne ou par le biais d'un réseau ou service de communications électroniques).

12. S'agissant du concept de « **criminalité grave** », l'Autorité observe que le droit belge applicable en la matière en consacre une **définition large.** L'article **127/1, § 1er, de la LCE** dispose que :

> « *Pour l'application du présent article, la criminalité grave comprend notamment les faits pour lesquels il existe des indices sérieux:*
>
> *1° qu'ils sont* ***de nature à entraîner la peine minimale d'emprisonnement correctionnel*** *principal visée à l'article 88bis, § 1er, alinéa 1er, du Code d'instruction criminelle* [soit **un emprisonnement correctionnel principal d'un an ou une peine plus lourde**];
>
> *2° qu'ils sont de nature à entraîner une sanction de niveau 5* [« la sanction de niveau 5 est constituée d'une amende pénale allant d'un montant **minimum de 250 euros à un montant maximum de 100 000 euros ou de 6 % du chiffre d'affaires** annuel total du dernier exercice clôturé précédant l'imposition de l'amende au sujet duquel des données permettant d'établir le chiffre d'affaires annuel sont disponibles, si cela représente un montant plus élevé, **et d'un emprisonnement d'un mois à un an ou d'une de ces peines seulement** »] *ou 6* [« la sanction de niveau 6 est constituée d'une amende pénale allant d'un montant **minimum de 500 euros à un montant maximum de 100 000 euros ou de 6 % du chiffre d'affaires** annuel total du dernier exercice clôturé précédant l'imposition de l'amende au sujet duquel des données permettant d'établir le chiffre d'affaires annuel sont disponibles, si cela représente un montant plus élevé, **et d'un emprisonnement d'un an à cinq ans ou d'une de ces peines seulement**] *visée à l'article XV.70 du Code de droit économique* ;
>
> *3° qu'ils pourraient constituer une infraction aux articles 14 ou 15 du règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ou aux dispositions prises sur la base ou en exécution de ces articles* » [(dispositions visant les **opérations d'initiés, la divulgation illicite d'informations privilégiées et les manipulations de marché**, sanctionnées sur le plan administratif en

droit européen, les Etats membres pouvant fixer des sanctions pénales (la LCE ne se réfère pas aux dispositions applicables en la matière)] » (mise en gras par l'Autorité).

13. L'Autorité est d'avis que l'on peut se questionner sur la mesure dans laquelle le droit belge ne vise pas également, en la matière, la criminalité ordinaire : **la notion retenue interroge au regard de la jurisprudence de la Cour de justice[2].** Et la **Cour constitutionnelle ne s'est pas prononcée sur la question de la constitutionnalité de l'article 127/1 de la LCE appliqué avec les dispositions régissant l'accès aux métadonnées de communications électroniques dans le cadre du Projet du Demandeur[3]**.

14. Cela étant précisé, **dans le cadre de la procédure pénale** (**hypothèse distincte du Projet**), la Cour constitutionnelle a jugé ce qui suit :

> « *B.102.1. En l'espèce, la partie requérante ne démontre pas en quoi le législateur aurait excédé la marge d'appréciation nationale en définissant, à l'article 39quinquies, § 1er, alinéa 1er, du Code d'instruction criminelle, la notion de « criminalité grave » par* ***référence aux infractions susceptibles de « donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde ». L'on n'aperçoit pas non plus en quoi cette définition violerait les normes de référence citées en B.99.2****. À cet égard, la section de législation du Conseil d'État a précisément observé, dans son avis sur l'avant-projet de loi qui est à l'origine de la loi du 20 juillet 2022, que « concernant le ministère public par exemple, le respect du critère de 'criminalité grave', résulte également de l'article 39quinquies en projet, du Code d'instruction criminelle » (Doc. parl., Chambre, 2021-2022, DOC 55-2572/001, p. 310). Du reste,* ***le rattachement d'une infraction pénale à la criminalité grave doit s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce****.*
>
> ***Le juge pénal doit en particulier être en mesure de refuser l'accès aux données concernées lorsque cet accès est sollicité dans le cadre de poursuites pour une infraction qui n'est manifestement pas grave*** *(CJUE, grande chambre, 30 avril 2024, C-178/22, précité, ECLI:EU:C:2024:371, point 62)* » (mis en gras et souligné par l'Autorité).

---

[2] Voir à ce sujet les avis suivants de l'Autorité et la jurisprudence de la Cour de justice qui y est citée : Avis n° 108/2025 du 17 octobre 2025 *concernant un projet d'arrêté royal établissant un cadre de référence pour la consultation des données ETIAS à des fins répressives (CO-A-2025-161)*, considérants nos 14-24 ; Avis n° 121/2023 du 18 juillet 2023 *concernant un avant-projet de loi relatif à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) (CO-A-2023-236) et un avant-projet de loi modifiant la loi relative à la création et à l'organisation des missions de l'Unité nationale ETIAS (U.N.E.) (CO-A-2023-237)*, considérants nos 92-93.

[3] Cour Const., arrêt n° 97/2024 du 26 septembre 2024, B.84.1-B.84.2, B.84.3, al. 2, B.87.3, B.88 et B.90.

15. Dans son arrêt, sur lequel la Cour constitutionnelle se base[4], **la Cour de justice a jugé ce qui suit** :

> « *54. À cet égard, il y a lieu de relever, premièrement, qu'une définition, selon laquelle les « infractions graves », pour la poursuite desquelles l'accès peut être octroyé, sont celles pour lesquelles la* ***peine de réclusion maximale est au moins égale à une durée que la loi détermine****, est fondée sur un* ***critère objectif****. Cela est conforme à l'exigence selon laquelle la législation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 105 ainsi que jurisprudence citée).*
>
> *55. Deuxièmement, il découle de la jurisprudence citée au point 48 du présent arrêt que la* ***définition donnée, en droit national, des « infractions graves »*** *pouvant permettre un accès aux données conservées par les fournisseurs de services de communications électroniques, permettant de tirer des conclusions précises sur la vie privée des personnes concernées,* ***ne doit pas être à ce point large que l'accès à ces données devienne la règle plutôt que l'exception. Ainsi, elle ne saurait couvrir la grande majorité des infractions pénales, ce qui serait le cas si le seuil au-delà duquel la peine de réclusion maximale dont est punie une infraction justifie que celle-ci soit qualifiée d'infraction grave était fixé à un niveau excessivement bas****.*
>
> *56. Or, un seuil fixé par* ***référence à une peine maximale de réclusion de trois ans n'apparaît pas, à cet égard, comme étant excessivement bas*** *(voir, en ce sens, arrêt du 21 juin 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, point 150).*
>
> *57. Certes, dès lors que la définition des « infractions graves », pour lesquelles l'accès aux données conservées par les fournisseurs de services de communications électroniques peut être demandé,* ***est établie par référence non pas à une peine minimale applicable mais à une peine maximale applicable, il n'est pas exclu qu'un accès à des données, constitutif d'une ingérence grave dans les droits fondamentaux, puisse être demandé à des fins de poursuites d'infractions ne relevant pas, en réalité, de la criminalité grave*** *(voir, par analogie, arrêt du 21 juin 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, point 151).*

[4] C.J.U.E. (Gr. Ch.), arrêt du 30 avril 2024, Procédures pénales c/Inconnus, Aff. C-178/22.

*58. La fixation d'un seuil à partir duquel la peine de réclusion maximale dont est punie une infraction justifie que celle-ci soit qualifiée d'infraction grave n'est toutefois pas nécessairement contraire au principe de proportionnalité.*

*59. D'une part, tel paraît être le cas d'une disposition telle que celle en cause au principal puisqu'elle vise, ainsi que cela ressort de la décision de renvoi, de manière générale, l'accès aux données conservées par les fournisseurs de services de communications électroniques, sans préciser la nature de ces données. Ainsi, cette disposition paraît couvrir notamment des cas dans lesquels l'accès ne peut être qualifié d'ingérence grave, car ne visant pas un ensemble de données susceptible de permettre de tirer des conclusions précises sur la vie privée des personnes concernées.*

*60. D'autre part,* ***la juridiction ou l'entité administrative indépendante, intervenant dans le cadre d'un contrôle préalable*** *effectué à la suite d'une demande d'accès motivée,* ***doit être habilitée à refuser ou à restreindre cet accès lorsqu'elle constate que l'ingérence dans les droits fondamentaux que constituerait un tel accès est grave alors qu'il est manifeste que l'infraction en cause ne relève pas effectivement de la criminalité grave*** *(voir, par analogie, arrêt du 21 juin 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, point 152).*

*61. En effet, la juridiction ou l'entité chargée du contrôle doit être en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès [arrêt de ce jour, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, point 125 ainsi que jurisprudence citée].*

*62. En particulier, dans le cadre de son examen de la proportionnalité de l'ingérence causée dans les droits fondamentaux de la personne concernée par la demande d'accès, cette juridiction ou cette entité* ***doit être en mesure d'exclure un tel accès lorsque ce dernier est sollicité dans le cadre de poursuites pour une infraction qui n'est manifestement pas grave****, au sens du point 50 du présent arrêt.*

*63. Il résulte de ce qui précède qu'il convient de répondre à la question préjudicielle que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il ne s'oppose pas à une disposition nationale qui impose au juge national, intervenant dans le cadre d'un*

*contrôle préalable effectué à la suite d'une demande motivée d'accès à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée d'un utilisateur d'un moyen de communication électronique, conservées par les fournisseurs de services de communications électroniques, présentée par une autorité nationale compétente dans le cadre d'une enquête pénale, d'**autoriser cet accès si celui-ci est demandé aux fins de la recherche d'infractions pénales punies, par le droit national, d'une peine de réclusion maximale d'au moins trois ans, sous réserve qu'il existe des indices suffisants de telles infractions et que ces données soient pertinentes pour constater les faits**, à condition, toutefois, que ce juge soit **habilité à refuser ledit accès si ce dernier est sollicité dans le cadre d'une enquête portant sur une infraction qui n'est manifestement pas grave**, au regard des conditions sociétales prévalant dans l'État membre concerné* » (mis en gras et souligné par l'Autorité).

16. **Transposées *mutatis mutandis* dans le cadre de la présente autorisation**, ces jurisprudences imposent à l'Autorité de vérifier si, concernant les adresses IP concernées, sont en cause des menaces graves pour la sécurité publique et/ou des infractions relevant de la criminalité grave au sens du cadre normatif applicable. Étant entendu qu'il convient dans ce contexte, de prendre également en compte la **finalité préventive** poursuivie par le CCB (CSIRT National) dans le cadre de son Projet et des règles qui s'y appliquent. En effet, ce dernier **ne s'inscrit pas dans le contexte d'une procédure pénale**. A l'inverse même, il se dégage explicitement de la Loi NIS2 que le Projet doit être sans finalité à caractère pénal.

17. Cela étant précisé, l'Autorité doit d'emblée concéder qu'elle n'est pas un acteur de la chaîne pénale (ministère public, juge d'instruction, juge du fond, etc.), ce qui rend à son niveau plus complexe la tâche d'évaluer si des faits potentiellement concernés sont de nature à entraîner la peine minimale d'emprisonnement correctionnel d'un an ou une peine plus lourde.

18. Quoi qu'il en soit, dans ce cadre général, et sans préjudice des autres développements de la présente Autorisation ainsi que des Autorisations précédentes de l'Autorité, le CCB (CSIRT National) **peut se limiter à étayer en fait, sur la base d'indices objectifs sérieux, la potentialité** que les adresses IP concernées soient utilisées afin de commettre, en Belgique, une infraction relevant de la **criminalité grave** au regard du droit applicable, ou de constituer, en Belgique, **une menace grave pour la sécurité publique**. A défaut, l'Autorité serait tenue de refuser l'accès aux métadonnées de communications électroniques dans le cadre des articles 126/1 et 127/1 de la LCE.

### II.3. Articles 126/1 et 127/1 de la LCE : application au Projet – menaces graves pour la sécurité publique et criminalité grave

19. Dans ce contexte, l'Autorité a interrogé le Demandeur afin qu'il identifie à quelle définition de « *menace grave pour la sécurité publique* » il est recouru dans le cadre du Projet (et sa source (jurisprudentielle ou doctrinale), et elle l'a invité, par *threat actor*, selon le fondement légal retenu, à identifier la menace grave pour la sécurité publique retenue et/ou l'infraction pénale relevant de la criminalité grave retenue (probablement, systématiquement et à tout le moins l'article 550*bis* et du Code pénal et de l'infraction d'espionnage – à charge pour le Demandeur d'en indiquer le fondement légal).

20. Elle l'a également interrogé sur les démarches entreprises afin de confirmer que les adresses IP concernées constituent bien des adresses dédiées au trafic de serveurs C2 engendrant de telles menaces (criminalité grave ou menace grave pour la sécurité publique). A cet égard, l'Autorité a observé que toutes les adresses concernées ont été identifiées par un partenaire privé du CCB (CSIRT National), [redacted], à l'exception d'une qui a été communiquée par [redacted]. Elle a également observé une relative diminution du détail des informations communiquées dans la Note contextuelle par rapport aux informations communiquées dans la Note de méthode (« Bijlage III – [redacted] », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT »), dans le cadre de l'Autorisation n° 001/2026.

21. Plus précisément à ce sujet, les questions suivantes ont été posées au CCB (CSIRT National) :

    - [redacted]
    - [redacted]
    - [redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

22. Le Demandeur a communiqué à l'Autorité des réponses étayées dans une note « Questions posées par l'APD dans le cadre du projet « Netflow » », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT » (ci-après, « **la Note de réponse** »). L'Autorité ne reprend pas exhaustivement cette note dans la présente Autorisation et se limite aux éléments repris ci-après.

### II.3.1. Relation avec des menaces graves pour la sécurité publique – cybermenaces concernées

23. S'agissant de la notion de **menace grave pour la sécurité publique**, le CCB (CSIRT National) indique notamment qu'il interprète cette notion comme « *comprenant toute circonstance, tout évènement ou toute action potentiels susceptibles d'avoir un impact important/grave sur la sécurité intérieure et extérieure de la Belgique, y compris sur les réseaux et systèmes d'information des entités essentielles ou importantes ou des utilisateurs (personnes morales ou personnes physiques) des services de ces entités* ».

24. L'Autorité en prend acte mais considère néanmoins, que la menace grave pour la sécurité publique dans le contexte normatif de la Loi NIS2 doit nécessairement être définie compte-tenu du champ d'application et des objectifs de la Loi NIS2. A ce sujet premièrement, elle doit se rapporter à une « **cybermenace** », s'agissant du type de menaces dont il est en l'occurrence systématiquement question. Comme l'indique le Demandeur, l'article 8, 10°, de la Loi NIS2 définit la cybermenace comme la cybermenace visée à l'article 2, 8), du Règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 *relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013*.

25. Deuxièmement, cette cybermenace est à lier à certains réseaux et systèmes d'information comme l'indique lui-même l'intitulé de la Loi NIS2 qui établit un cadre pour la cybersécurité des réseaux et des systèmes d'information *d'intérêt général pour la sécurité publique*. Autrement dit, la Loi NIS2 vise certains réseaux et systèmes d'information qui sont considérés comme d'intérêt général pour la sécurité publique.

26. Dans ce contexte, l'Autorité considère que, pour que les métadonnées relatives au trafic depuis et vers une adresse IP concernée puissent être collectées en raison de la relation entre cette adresse et une menace grave pour la sécurité publique, cette adresse doit être liée à « *toute circonstance, tout*

*événement ou toute action potentiels susceptibles de nuire gravement/de manière importante ou de porter autrement atteinte gravement/de manière importante aux réseaux et systèmes d'information des entités essentielles ou importantes ou aux utilisateurs (personnes morales ou personnes physiques) des services de ces entités* ».

27. Quant au questionnement soulevé par l'Autorité concernant [redacted], et le lien entre ces adresses IP et la menace grave pour la sécurité publique, **le Demandeur a notamment communiqué les éléments pertinents et convaincants suivants,** dans sa Note de réponse :

> « *La protection des réseaux et systèmes d'informations* ***des entités NIS2*** *(essentielles qui sont en principe les grandes entreprises actives dans les secteurs très critiques de l'annexe I de la loi et importantes qui sont en principe les moyennes entreprises actives dans les secteurs très critiques de l'annexe I et les moyennes et grandes entreprises actives dans les autres secteurs critiques de l'annexe II de la loi) contre les menaces graves qui émanent de serveurs C2 est un enjeu directement lié à la sécurité publique, étant donné l'impact potentiel des activités de ces acteurs malveillants sur la sécurité publique de la Belgique.*
>
> *Un serveur C2 est une infrastructure technique opérationnelle permettant à un acteur malicieux de maintenir un accès au sein d'un système informatique, y déployer des outils offensifs ou encore y exfiltrer des données.* [redacted]

[redacted]

*Dans ce contexte,* ***la recherche active de la présence de serveurs C2 ou de signes de compromissions constitue une mesure préventive pour assurer la sécurité publique****.* ***Attendre une perturbation visible reviendrait à intervenir trop tard****, lorsque l'acteur aurait déjà acquis l'accès, les connaissance et capacités nécessaires pour perturber les systèmes informatiques.* [redacted]

*C'est dans ce cadre spécifique que s'inscrit le projet.* ***Ce raisonnement s'applique à l'ensemble des adresses IP repris sur la liste communiquée et aux adresses IP qui seront communiquées dans le cadre de demandes subséquentes****. De par les éléments décrits ci-avant, chaque serveur C2 sélectionné minutieusement par les analystes du CCB pour être inclus sur la liste constitue une menace grave pour la sécurité publique* » (mis en gras et souligné par l'Autorité).

28. L'Autorité prend acte de **cette motivation qui peut être retenue dans le cadre des adresses IP identifiées dans la présente Demande** [redacted]

29. 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 [redacted] 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 [redacted].).

30. Cela étant précisé, il n'est *a priori* pas exclu qu'à l'avenir, d'autres menaces graves pour la sécurité publique soient susceptibles d'être identifiées, selon les acteurs de la menace concernés [redacted]

[redacted]

[redacted] Le Demandeur devra y prêter attention dans le cadre de ses demandes ultérieures (d'autorisation préalable ou de contrôle ultérieur).

**II.3.2. Relation avec la criminalité grave**

31. Dans sa Note de réponse, le Demandeur a communiqué à l'Autorité une **liste** de [redacted] infractions ainsi que leurs références dans le nouveau Code pénal en précisant que cette liste **s'applique pour chaque adresse IP/acteur malveillant repris(e) sur la liste**. Le Demandeur précise néanmoins ce qui suit, et il convient effectivement d'apporter cette nuance liée à la nature préventive du Projet : [redacted] (mise en gras modifiée par l'Autorité).

32. De nouveau (voir le considérant n° 28), une attention particulière doit par conséquent notamment (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) être réservée à la **description de l'acteur (ou du moyen) de la menace concerné** sur la base de sources fiables, de telle sorte qu'effectivement, des indices sérieux indiquent la potentialité d'un lien entre les adresses IP concernées et la criminalité grave.

33. Quant à cette dernière, **le Demandeur se limite à lister les infractions suivantes qui seraient applicables à toutes les adresses IP** : « [redacted]

[redacted]

34. **L'Autorité ne poursuit pas plus loin l'analyse de la relation entre les adresses IP communiquées et la criminalité grave**.

35. En effet, d'une part, dès lors qu'elle reconnaît déjà que les adresses IP communiquées peuvent être considérées comme étant relatives à des menaces graves contre la sécurité publique, **le CCB (CSIRT National) peut déjà se prévaloir** des articles 126/1, § 1er, al. 3, et 127/1, § 2, 2°, de la LCE, et 21, § 2, 2°, de la Loi NIS2 **pour fonder la collecte des métadonnées de communications électroniques souhaitées**.

36. D'autre part, l'Autorité considère que **la motivation communiquée par le Demandeur en la matière devrait être adaptée**. **Certes, l'Autorité perçoit bien qu'il est question d'activités d'une gravité certaine**, comme en attestent les développements précédents qui reconnaissent que les activités concernées constituent une menace grave pour la sécurité publique. Mais il ne suffit pas en l'occurrence de communiquer à l'Autorité une liste d'infractions systématiquement susceptibles de se produire dans toutes les hypothèses sans motivation concrète relative à chacune des adresses IP concernée, et de surcroît sans motivation particulière indiquant que les faits concernés sont bien

susceptibles d'une peine d'emprisonnement d'un an ou d'une peine plus lourde (sauf à identifier en tant que telles, les infractions concernées dont le minimum de la peine est déjà d'un an d'emprisonnement). Par ailleurs, le demandeur se fonde sur les dispositions du nouveau Code pénal qui n'est *a priori* pas encore entré vigueur[8].

37. L'Autorité considère que pour lier une adresse IP à la criminalité grave au sens du droit applicable, il n'est pas nécessaire de lister l'ensemble des infractions susceptibles de se produire via celle-ci, mais il convient, **dans la Note contextuelle, dans les développements dédiés à cette adresse IP,** de **lier concrètement et de manière convaincante cette adresse à des faits susceptibles de constituer une ou de plusieurs infractions pertinentes passibles des peines pertinentes** – il s'agit d'une motivation de droit pénal.

38. Pour le surplus, cette motivation peut être réalisée, *mutatis mutandis*, à la manière dont les adresses IP seraient liées à des menaces graves contre la sécurité publique (**considérant n° 29**). Ainsi, compte-tenu de la **finalité préventive** du Projet, la relation entre l'adresse IP concernée et de tels faits 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 sérieux, à des faits relevant de la criminalité grave ; et/ou

- Il existe des indices sérieux sur la base desquels **l'adresse IP concernée** a été utilisée en relation avec de tels faits.

39. Il appartient dans ce contexte au CCB (CSIRT National) de choisir le fondement le mieux adapté au regard des serveurs C2 concernés et de motiver sa Demande en conséquence.

### II.3.3. Indices sérieux et vérifications réalisées par le CCB (CSIRT National)

40. Comme indiqué précédemment, [redacted] les [redacted] adresses IP identifiées dans le cadre de la Demande sont toutes retenues sur la base d'informations communiquées par [redacted] Comme cela était prévu dans les Autorisation précédentes, chaque adresse IP a notamment été l'objet d'une [redacted]

[8] Voir https://justice.belgium.be/fr/nouvelles/autres_communiques/nouveau_code_penal_entree_en_vigueur_reportee, dernièrement consulté le 16/06/2026.

[redacted] réalisée par le CCB (CSIRT National). Interrogé à ce sujet[9], le CCB (CSIRT national) a notamment précisé ce qui suit :

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

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

[9] Voir le considérant n° 21.

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

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

41. L'Autorité prend acte de cette réponse. Elle note qu'effectivement, dans la logique des Autorisations préalables et de l'approche que le CCB (CSIRT National) entend poursuivre dans le cadre de son Projet et de l'exécution de sa mission d'intérêt public, [redacted], et ce, afin de pouvoir mieux endiguer les menaces concernées en [redacted] (voir les **considérants nos 43-44 de l'Autorisation n° 001/2026**). **Ce qui rend <u>d'autant plus importantes et déterminantes</u> les**

**informations et vérifications sur la base desquelles le CCB (CSIRT National) valide les adresses IP retenues**.

42. A cet égard, **afin de pouvoir réaliser un contrôle effectif, l'Autorité** :

- Attend du Demandeur que les demandes ultérieures (d'autorisation préalable ou de contrôle ultérieur) **continuent d'être accompagnées 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 présente Demande, **le cas échéant précisée** à l'aune des considérations développées dans les **considérants nos 23-39**) ;

- Cette note doit également **indiquer explicitement** [redacted] Cette note **doit en outre indiquer les résultats de ces analyses**, positifs ou négatifs, selon que la recherche confirme ou infirme respectivement, que l'adresse IP est [redacted] ;

- Afin de limiter au maximum la charge administrative du CCB (CSIRT National) dans le cadre des demandes d'autorisation (ou de contrôle) ultérieures dans le cadre du Projet, l'Autorité planifie de **se limiter en outre**, à la manière dont elle a procédé dans le cadre de la présente Demande, à **ne sélectionner qu'un échantillon d'une (ou plus) adresse(s) IP** pour la(les)quelle(s) le CCB (CSIRT National) serait invité, au regard de la réponse communiquée et reprise au **considérant n° 40**, à communiquer les **informations complémentaires suivantes** : [redacted] les autres informations éventuellement utilisées ainsi que l'éventuelle enquête subséquente mise en œuvre. Cela étant dit, il va de soi que **si le Demandeur le souhaite, il est lui est loisible de communiquer d'initiative l'ensemble de ces informations, le cas échéant sous une forme brute**. Dans une telle hypothèse, l'Autorité n'aurait pas besoin de sélectionner une ou plusieurs adresses IP à propos desquelles il y aurait lieu de communiquer des informations complémentaires, **ce qui pourrait accélérer le processus d'autorisation**.

43. Dans ses réponses, le CCB (CSIRT National) indique également que « *We hebben besloten de aan de gegevensbeschermingsautoriteit verstrekte informatie te beperken tot de meest essentiële elementen* ». L'Autorité souligne, en comparaison avec les éléments communiqués dans le cadre de la demande précédente, que si une telle limitation peut en pratique, dans une certaine mesure, limiter la charge administrative du CCB (CSIRT National), elle peut néanmoins soulever des interrogations de la part de l'Autorité. L'objectif à atteindre demeure d'étayer au mieux les demandes d'autorisation dès leur introduction, en recherchant un juste équilibre entre la charge administrative que cela implique pour le CCB (CSIRT National) et l'obligation de l'Autorité d'exercer un contrôle rapide et effectif.

44. L'Autorité est bien consciente du **temps que nécessite le processus d'autorisation** (préparation de la Demande, analyse de celle-ci par l'Autorité, décision) dans le cadre duquel elle doit réaliser un contrôle du traitement de données envisagé. L'Autorité **attire néanmoins l'attention du Demandeur sur les points suivants.** La première demande introduite par le CCB (CSIRT National) a nécessité une première étude approfondie du Projet concerné, tant sur le plan juridique que sur le plan technique, notamment afin que l'Autorité puisse comprendre correctement la manière dont travaille le CCB (CSIRT National) dans ce contexte. Chaque Demande ultérieure a comporté une modification nécessitant une analyse complémentaire sur le plan juridique, de telle sorte notamment, que les Demandes n'ont pas pu être introduites dans le cadre d'un contrôle ultérieur (voir à ce sujet les **considérants nos 18-24 de l'Autorisation n° 001/2025**) (à supposer pour le reste, que l'urgence soit rencontrée *in concreto*). Chaque Demande a nécessité des questions complémentaires de la part de l'Autorité également sur le plan technique, le cas échéant afin de contrôler *in concreto* l'existence de suffisamment d'informations (indices sérieux) pour lier chaque adresse IP à un serveur C2 et à la menace alléguée, ou pour confirmer/préciser/adapter les mesures de vérification mises en œuvre. Une fois de plus, l'objectif est pour l'Autorité de pouvoir vérifier et bien comprendre les méthodes de travail du CCB (CSIRT National). Dans ce contexte, si le Projet ne change pas et que suffisamment d'informations (éléments de preuve/d'analyse) sont d'emblée directement communiquées à l'Autorité, la décision sur l'autorisation demandée devrait être délivrée plus rapidement. Une fois en possession des informations nécessaires, l'Autorité s'est chaque fois prononcée à très court délais. Enfin, en cas d'urgence avérée, l'Autorité peut toujours être consultée dans le cadre d'un contrôle ultérieur plutôt que sur autorisation préalable, de telle sorte que la mise en œuvre de son contrôle par l'Autorité ne pourra pas, en pratique, empêcher la réaction face à une menace actuelle et imminente. Le coût des démarches précitées est celui de l'exercice d'une compétence qui entraîne une ingérence dans la confidentialité des métadonnées de communications électroniques traitées par les opérateurs.

45. Enfin, l'Autotrié 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 [redacted]. Il s'agit d'une mesure pertinente et importante qui aurait gagné à être

d'emblée mise en évidence. Elle prend également acte du fait que [redacted] (le Demandeur a communiqué à cet égard à l'Autorité une illustration concernant une des adresses IP).

## II.4. Périodes couvertes par les métadonnées concernées

46. En ce qui concerne les données qui sont conservées par les opérateurs en application des **articles 122 et 123 de la LCE**, l'Autorité se réfère aux **considérants 19-28 de son Autorisation n° 001/2026**.

47. L'article 126/1, § 1er, al. 1er, de la LCE prévoit que les « *opérateurs conservent les données visées à l'article 126/2, § 2, pour les zones géographiques visées à l'article 126/3, pendant* ***douze mois à partir de la date de la communication, sauf si une autre durée est fixée dans l'article 126/3*** » (mis en gras par l'Autorité). L'article 126/3 de la LCE identifie différentes zones géographiques pour lesquelles doivent être conservées les métadonnées de communications électroniques. En substance :

- L'article 126/3, **§ 1er**, al. 1er, de la LCE détermine deux types de zones géographiques (arrondissements judiciaires et zones de police) pour lesquelles les métadonnées de communications électroniques doivent être conservées en fonction de la commission de certaines infractions par mille habitants par an (en moyenne sur trois ans), et ses alinéas 2 et 3 fixent les durées de conservation des métadonnées dans ces cas, à **6, 9 ou 12 mois** selon le nombre d'infractions concerné ;

- L'article 126/3, **§ 2**, de la LCE vise des zones géographiques (le cas échéant, l'ensemble du territoire) **identifiées par l'Organe de coordination pour l'analyse de la menace** et pour lesquelles un certain niveau de menace est retenu (3). Dans ces zones, les métadonnées doivent être conservées **aussi longtemps que le niveau de la menace est d'au moins 3** ;

- L'article 126/3, **§ 3**, de la LCE vise toute une série de « *zones particulièrement exposées à des menaces pour la sécurité nationale ou à la commission d'actes de criminalité grave* », dont les gares, les prisons, les stations de métro, les aéroports, les armuriers et les stands de tir, les communes dans lesquelles des infrastructures critiques se trouvent, etc. Le Roi en fixe le périmètre. Ces métadonnées doivent *a priori* être conservées **12 mois**, conformément à l'article 126/1, § 1er, al. 1er, de la LCE ;

- L'article 126/3, **§ 4**, de la LCE vise les « *zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population* », à savoir, par exemple les autoroutes et les parkings publics attenants, les assemblées législatives, les maisons communales et les hôtels de ville, etc. Le Roi en fixe le périmètre. Ces métadonnées doivent *a priori* être conservées **12 mois**, conformément à l'article 126/1, § 1er, al. 1er, de la LCE ;

- L'article 126/3, **§ 5**, de la LCE, vise « les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales établies sur le territoire national », à savoir notamment, les ambassades, les bâtiments affectés à l'Union européenne, etc. Le Roi en fixe le périmètre. Ces métadonnées doivent *a priori* être conservées **12 mois**, conformément à l'article 126/1, § 1er, al. 1er, de la LCE.

48. Il **incombe au CCB (CSIRT National) de veiller à ce que les dates *first seen*** identifiées dans la Note contextuelle communiquée par le CCB (CSIRT National) **entrent bien dans les périodes couvertes par l'obligation de conservation des métadonnées précitées, à compter de la date de la présente décision**. A défaut, il conviendra de retenir une date ultérieure (tout en conservant bien entendu également la date *first seen* initialement retenue).

49. A cet égard, **l'Autorité attire l'attention du Demandeur sur les adresses IP suivantes** dont les dates *first seen* remontent à plus de douze mois – les références ci-après sont construites comme suit : [redacted]

50. Enfin, l'Autorité souligne que conformément au **principe d'*accountability*** (articles 5, 2., et 24 du RGPD), le CCB (CSIRT National) doit être capable de justifier du fondement légal sur la base duquel les métadonnées communiquées effectivement par un opérateur étaient conservées par celui-ci (cette obligation incombe également à l'opérateur concerné qui est responsable du traitement de conservation des métadonnées) – articles 122 et 123, ou articles 126/1 et 127/1 de la LCE. Dans le cadre de l'Autorisation n° 001/2026 par exemple, le CCB (CSIRT National) n'a pas été en mesure d'indiquer combien de temps les opérateurs conservaient les métadonnées de communications électroniques pour leurs propres finalités (voir le considérant n° 26 de l'Autorisation n° 001/2026). Or en pratique, lorsque celles-ci seront communiquées au CCB (CSIRT National), ce dernier doit être en mesure d'identifier sur quel fondement légal celles-ci étaient conservées.

### II.5. 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 s'aligner entièrement sur les éléments soulevés dans l'Autorisation n° 001/2026 (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 23-39 et 46-50**) :

- 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 ;

- 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.

**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**).

**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 la présente Autorisation), 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 présente Demande, le cas échéant précisée à l'aune des considérations développées dans les considérants nos 23-39. [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**) ;

**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) [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 23 adresses IP dédiées à des C2-servers contextualisées dans la Note contextuelle et reprises en Annexe 1 (lignes nos 9-31 incluse), à partir des dates « *first seen* » le cas échéant adaptées, 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

**SENSIBLE NON CLASSIFIE (AR 20.12.2024)**

[redacted]