Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 230/2026 du 27 octobre 2026

Objet : avis concernant un Projet de loi *transposant la directive (UE) 2023/977 du Parlement européen et du Conseil du 10 mai 2023 relative à l'échange d'informations entre les services répressifs des États membres et abrogeant la décision-cadre 2006/960/JAI du Conseil* (ADV-2026-00192).

Mots-clés : prévention et détection des infractions pénales ; coopération internationale dans le domaine pénal ; échanges de données intra européens par les services répressifs ; douanes et accises ; compétence de l'Autorité.

Version originale

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier ses articles 23 et 26 (ci-après « LCA ») ;

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 « 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 « LTD ») ;

Vu la demande d'avis de Monsieur Peter De Roover (ci-après « le Demandeur »), Président de la Chambre des représentants, reçue le 14 octobre 2026 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 27 octobre 2026, l'avis suivant :

L'Autorité ne publie en français et en néerlandais que les avis concernant les projets ou propositions de textes de rang de loi émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale ou de la Commission Communautaire Commune. La « Version originale » est la version qui a été validée.

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Demandeur a introduit auprès de l'Autorité une demande d'avis en urgence (à émettre dans les 5 jours ouvrables) concernant un Projet de loi[1] *transposant la directive (UE) 2023/977 du Parlement européen et du Conseil du 10 mai 2023 relative à l'échange d'informations entre les services répressifs des États membres et abrogeant la décision-cadre 2006/960/JAI du Conseil* (ci-après, « **le Projet** », « **la Directive** » et la « **Décision JAI** »).

2. S'agissant de **l'urgence**, l'article 48 du Règlement d'ordre intérieur de l'Autorité[2] dispose que :

> « ***A peine d'irrecevabilité,*** *toute demande d'avis sollicitée dans l'urgence est spécifiquement motivée dans un champ dédié du formulaire de demande d'avis. Cette motivation doit comporter les motifs pour lesquels le demandeur ne peut attendre un délai plus long que 5 ouvrables pour disposer de l'avis. Ces motifs doivent être précis, concrets et* ***justifier de l'imprévisibilité de la situation*** *à laquelle le demandeur est confronté. Le Service estime que seule une situation de cas de force majeure (****situation imprévisible et non imputable en tout ou en partie au demandeur d'avis****) générant une telle situation d'urgence pourra justifier une telle saisine. Ainsi, notamment, l'intérêt général lié à l'aboutissement du dossier, ne peut à lui seul justifier l'urgence.* ***Il en est de même du dépassement avéré ou imminent du délai de transposition d'une directive européenne*** » (mis en gras par l'Autorité).

3. L'Autorité observe que le Conseil d'Etat et l'Organe de Contrôle de l'Information Policière (ci-après, « **le COC** ») ont été saisis le 2 février 2026 et ont respectivement rendu les Avis n° 78.857/2 du 3 mars 2026 et n° DA260006 du 1er avril 2026 (ci-après, « **l'Avis du COC** »). Le Demandeur justifie de l'urgence dans le formulaire de demande d'avis en ces termes :

> « *La Belgique fait l'objet d'une procédure d'infraction pour défaut de* ***transposition*** *de la directive (UE) 2023/977, dont le* ***délai a expiré le 12 décembre 2024.*** *La Commission européenne a déjà différé sa décision quant à une éventuelle saisine de la Cour de justice de l'Union européenne et réexaminera la situation belge à la mi-novembre 2026.*
> ***La nécessité de consulter l'APD n'a été identifiée que tardivement****, lors de l'examen juridique du projet par les services de la Chambre. Cette consultation n'avait été relevée ni dans la note au Conseil des ministres, ni lors des examens par le Conseil d'État et le COC.*

---

[1] *Doc. Parl.*, Ch. des représentants, DOC n° 56 1665/001.

[2] Disponible sur https://www.autoriteprotectiondonnees.be/publications/reglement-d-ordre-interieur-de-l-autorite-de-protection-des-donnees.pdf.

La Chambre a déjà accepté de traiter le projet en urgence afin de permettre sa transposition avant la prochaine échéance européenne.
Le délai ordinaire de consultation de l'APD (30 jours) risquerait de compromettre l'achèvement des travaux parlementaires avant cette échéance et d'accroître le risque d'une saisine de la Cour de justice ».

4. Tant l'obligation de consulter l'Autorité que le délai de transposition de la Directive sont prévisibles de telle sorte que l'auteur du Projet et le Demandeur ne peuvent se prévaloir d'une situation imprévisible justifiant l'introduction d'une demande d'avis à traiter dans les cinq jours ouvrables. **Le traitement de la Demande d'avis en urgence n'est par conséquent pas accordé**. Ce qui n'exclut pas que consciente de la situation dans laquelle se trouve le Demandeur, l'Autorité a fait en sorte d' agir dans les meilleurs délais.

II. EXAMEN DU PROJET

Le présent avis est structuré comme suit :

II.1. Le Projet 3
II.2. Droit de la protection des données applicable, compétence de l'Autorité et champ d'application du Projet 5
II.3. Absence de « mesures coercitives » et autorisations judiciaires éventuellement nécessaires ... 10
II.4. Protection des données et motifs de refus des demandes d'informations 13
II.5. Exactitude et caractère à jour des données 18
II.6. Responsabilités au regard des traitements de données 19

II.1. Le Projet

5. En quelques mots, le Projet régit, en exécution de la Directive, les échanges de données qui revêtent un intérêt pour les services répressifs aux fins de l'accomplissement des missions de prévention, de détection ou de répression des infractions pénales entre autorités répressives des Etats membres (pour le moment, la police et la douane concernant la Belgique). Il crée un point de contact unique à cette fin (un « **SPOC** ») au sein de la Direction de la coopération policière internationale de la police fédérale et la mise en place d'un système de gestion des dossiers.

6. En quelques mots, il est prévu que « *les informations disponibles* » puissent être en principe échangées entre SPOC à l'attention des services répressifs compétents. Un SPOC d'un Etat membre peut égale-

ment adresser une demande à un service répressif belge et exceptionnellement (urgence opérationnelle) ce service pourra lui répondre directement. Tout aussi exceptionnellement (urgence opérationnelle), les services répressifs pourront également échanger directement les informations recherchées. Dans tous les cas, l'échange d'informations doit avoir lieu à des conditions équivalentes à celles applicables pour demander ou communiquer des informations similaires en Belgique[3]. L'échange d'informations a lieu sur demande (Chapitres VI à VIII du Projet) ou sur propre initiative (Chapitre IX du Projet) et ce, via le système sécurisé d'EUROPOL « *Secure Information Exchange Network Application* » (ci-après, « **SIENA** »). Exceptionnellement (notamment en cas d'urgence opérationnelle lorsque les services répressifs s'échangent directement les informations), un autre canal temporaire pourrait être utilisé.

7. **Quant à son champ d'application, la Directive va plus loin que la Décision JAI qu'elle remplace** en ce que d'une part, elle est désormais également applicable à l'échange d'informations en vue de la **« *prévention* »** des infractions pénales et en vise plus largement la « *détection* », sans définir ces concepts, alors que la Décision JAI visait les « *enquêtes pénales* » ou les « *opérations de renseignement en matière pénale* » dont elle consacrait les définitions[4, 5] (les développements ultérieurs se réfèreront à cette finalité par les termes « **aux fins concernées** »). La Directive vise d'autre part désormais plus largement **les infractions pénales en général**, au sens du droit européen[6], alors que la décision JAI ne visait qu'une liste d'infractions qu'elle énumérait. En substance, elle **raccourcit également les délais** dans lesquels les services répressifs concernés doivent répondre. L'article 12, § 1er, du Projet prévoit que le SPOC doit répondre dans les **8 heures** pour les demandes urgentes sur des informations directement accessibles, dans les **3 jours civils** pour les demandes urgentes portant sur des informations indirectement accessibles et dans les **7 jours civils** pour toutes les autres demandes, une dérogation étant possible en cas de nécessité d'une autorisation judiciaire.

---

[3] Article 6 du Projet.

[4] Voir son article 1er, 1. Ces concepts sont définis dans l'article 2, b) et c) de la Décision JAI.

[5] L'exposé des motifs indique par exemple ce qui suit :

« *Alors que la décision-cadre suédoise ne portait que sur l'échange international d'informations entre les États membres dans le cadre d'une enquête pénale ou d'une opération de renseignement, la directive (UE) 2023/977 s'applique désormais aussi à la prévention d'infractions. Il en résulte que l'échange international d'informations au titre du présent projet de loi peut porter tant sur des informations de police judiciaire que, dans certains cas, désormais aussi sur des informations de police administrative. Des informations indiquant, par exemple, que certaines personnes identifiées vont assister à un événement et qu'il y a des motifs raisonnables de croire qu'elles pourraient commettre une infraction, devront dorénavant être échangées conformément aux règles décrites ci-après, étant donné qu'il s'agit de la prévention d'infractions. Toutefois, s'il s'agit d'informations de police administrative plus générales concernant l'organisation d'un événement, celles-ci pourront toujours être échangées directement entre les points de contact spécialement prévus à cette fin* ».

[6] Le considérant n° 11 de la Directive indique que :

« *L'expression «infraction pénale» est une notion autonome du droit de l'Union tel qu'il est interprété par la Cour de justice de l'Union européenne. Aux fins de la présente directive, dans l'intérêt d'une lutte efficace contre la criminalité, il convient d'entendre par «infraction pénale» **tout comportement punissable en vertu du droit pénal de l'État membre qui reçoit des informations**, soit à la suite d'une demande, soit à la suite d'une communication d'informations sur propre initiative conformément à la présente directive, quelle que soit la sanction pouvant être infligée dans cet État membre et indépendamment de la question de savoir si le comportement est également punissable en vertu du droit pénal de l'État membre qui communique des informations, sans préjudice des motifs de refus des demandes d'informations énoncés dans la présente directive* » (mis en gras par l'Autorité).

II.2. Droit de la protection des données applicable, compétence de l'Autorité et champ d'application du Projet

8. Sur le plan de la protection des données à caractère personnel, la Directive s'inscrit dans le champ d'application de la Directive (UE) n° 2016/680 *du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil*, (ci-après, « **la Directive 2016/680** »)[7] transposée en droit belge dans le **Titre 2 de la LTD**. Le législateur belge a choisi d'énumérer explicitement et limitativement les autorités compétentes soumises au champ d'application de ce Titre[8]. La Directive 2016/680 quant à elle, suit une approche fonctionnelle de la définition des autorités concernées et s'applique au traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces[9]. De telle sorte qu'il n'est pas exclu que des autorités belges qualifiables d'autorités compétentes au sens de la Directive 2016/680 soient néanmoins exclues du champ d'application du Titre 2 de la LTD – auquel cas elles seront soumises au RPGD.

9. S'agissant de la compétence des autorités de contrôle, **l'Autorité jouit en droit belge d'une compétence[10] générale[11] et résiduaire[12]**. Selon les responsables du traitement et selon les traitements

---

[7] Outre l'applicabilité de la Directive 2016/680 découlant de son propre champ d'application, voir également les considérants nos 23,34 et 39, ainsi que les articles 2, 8), 6, 1., e), 10, a), 15, 3., et 16, 1., h), de la Directive.

[8] Voir l'article 26, 7°, de la LTD.

[9] Voir les articles 1, 1., et 3, 7., de la Directive n° 2016/680.

Les autorités compétentes sont définies par cette dernière disposition comme :

« *a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou*

b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ».

S'agissant par exemple de l'oubli des établissements pénitentiaires, voir l'Avis n° 89/2025 du 25 septembre 2025 *concernant un Avant-projet de loi relative aux tests de drogue dans les maisons de transition et à la déchéance de nationalité belge (CO-A-2025-097)*, considérants nos 5-6.

[10] Voir notamment, le Protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données, *Convention entre l'Autorité de Protection des données, l'Organe de Contrôle de l'Information Policière, le Comité Permanent de contrôle des services de renseignement et le Comité Permanent de contrôle des services de police*, 24 novembre 2020, p. 10, disponible sur https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-controle-federales-belges-en-matiere-de-protection-des-donnees.pdf, dernièrement consulté le 16/10/2026.

[11] Article 4, § 1er, de la LCA.

[12] Article 4, § 2, al. 2, de la LCA.

de données concernés, **elle appliquera le RGPD et le Titre 1er de la LTD, ou le Titre 2 de la LTD**, par exemple s'agissant de l'Administration générale des douanes et accises, qui est directement visée par le Projet (ci-après « **l'AGD&A** »), et de l'Office des Etrangers[13].

10. L'Autorité rappelle encore, s'agissant des **autorités judiciaires**, qu'elle est bien compétente pour rendre un avis à l'égard du Projet et de tout projet de norme qui concernerait le traitement de données à caractère personnel par ces autorités[14]. L'article 55, 3., du RGPD ne limite pas sa compétence en la matière. L'Autorité souligne de nouveau qu'aucune autorité n'est compétente en droit positif belge, pour *contrôler* la conformité des traitements dont sont responsables les autorités judiciaires, aux règles de protection des données. Dans le cadre du Projet, les autorités judiciaires sont susceptibles d'être impliquées lorsqu'un échange d'informations nécessite leur **autorisation**[15].

11. L'article 2, 1), de la Directive, définit le « ***service répressif compétent*** » comme « *tout service de police, de douanes ou autre des États membres* ***compétent en vertu du droit national pour exercer son autorité et prendre des mesures coercitives aux fins de la prévention ou de la détection des infractions pénales, ou des enquêtes en la matière****, ou toute autorité qui* ***participe à des entités conjointes*** *créées entre deux États membres ou plus* ***aux fins de la prévention ou de la détection des infractions pénales ou des enquêtes en la matière****, à l'exclusion des agences ou unités traitant particulièrement des questions de sécurité nationale et des fonctionnaires de liaison détachés en vertu de l'article 47 de la convention d'application de l'accord de Schengen* »[16] (mis en gras par l'Autorité).

12. L'article 4, 2°, du Projet, définit le « *service répressif belge* » comme « *un des* ***services de police*** *tels que visés à l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les* ***services de recherche de l'Administration générale des Douanes et Accises*** *ainsi que* ***tout service désigné comme tel par le Roi*** » (mis en gras par l'Autorité). L'exposé des motifs indique ainsi que « *La police, la douane* ***et les autres services répressifs*** *vont*

---

[13] Voir encore récemment à ce sujet, l'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 4-8.

[14] Voir notamment : Avis n° 77/2020 du 24 août 2020 *concernant une proposition de loi contenant le Code de procédure pénale (CO-A-2020-059)*, considérants nos 7-14 et ; Avis n° 163/2023 du 18 décembre 2023 *concernant un avant-projet de loi portant statut social du magistrat (CO-A-2023-465)*, considérants nos 5-9.

[15] Voir les considérants nos 25-31.

[16] L'exposé des motifs précise encore ce qui suit :

« *Le concept de "****service répressif désigné"*** *(1°) a été introduit par la directive (UE) 2023/977 pour répondre aux souhaits de* ***certains États membres dont la structure est très décentralisée*** *(par exemple, la Suisse et l'Allemagne). Ces services répressifs désignés peuvent, à l'instar d'un point de contact unique, adresser une demande d'informations aux points de contact uniques des États membres. En Belgique, aucun service répressif désigné n'est nommé compte tenu des obligations légales et de la politique centrale en matière d'échange international d'informations*[…] *visant, par la coordination des informations, les recoupements et le contrôle qualité, à éviter les flux d'informations parallèles* […]

Le ministère public n'est pas un service répressif *belge dans le cadre du présent projet de loi. La directive (UE) 2023/977 n'a en effet voulu créer aucune obligation pour les autorités judiciaires étant donné que celles-ci ne participent pas directement à l'échange international d'informations policières* » (mis en gras par l'Autorité).

encore renforcer leur coopération au sein de l'Union en vue de lutter contre la criminalité » (mis en gras par l'Autorité).

13. Sur ce point premièrement, l'Autorité est d'avis que c'est **au Projet lui-même (soit une norme du rang de loi)** d'être adapté dans le cas où il serait envisagé d'étendre son application à d'autres services répressifs. En effet, la détermination du champ d'application du Projet quant aux services répressifs concernés est à tout le moins **déterminante, sur le plan de la protection des données** : dans la détermination de la finalité des traitements de données (les accès du service répressif concerné sont désormais utilisés aux fins de la Directive et du Projet) ; dans l'identification des responsables du traitement (ces services) ; dans l'identification des destinataires des données et des catégories de données concernées (les données traitées par les services belges concernés pourront être communiquées en vertu du Projet à des homologues européens) ; dans l'identification des catégories de données traitées (les données traitées par les services concernés pourront être communiquées à d'autres services répressifs européens en vertu du Projet). Or conformément aux principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution, les **éléments essentiels des traitements de données doivent être fixés dans une norme du rang de loi**[17].

14. Deuxièmement, l'Autorité relève la position tout à fait pertinente exprimée par le COC aux considérants nos 16 à 16.3 de son avis, selon laquelle la Directive devrait plutôt à être transposée dans la **Loi du 5 août 1992 *sur la fonction de police*** (ci-après, « **la LFP** »), s'agissant de règles régissant le traitement de l'information policière. Cela étant dit, le Projet s'applique aussi à l'AGD&A et s'il était envisagé d'étendre le champ d'application du Projet à d'autres services « répressifs » parmi les nombreux services de contrôle et d'inspection, potentiellement régionaux également[18], qui existent en droit belge et sont impliqués dans la prévention et la détection d'infractions pénales, l'existence d'une loi spécifique demeurerait d'autant plus pertinente, la LFP n'ayant pas vocation à s'appliquer à ces autres entités. Cela étant précisé, l'exposé des motifs ne révèle aucune information quant à la possibilité d'étendre l'application du Projet à d'autres services répressifs belges.

15. **S'agissant des informations disponibles concernées**, le Projet s'applique **au-delà des banques de données policières**, en ce qu'il définit ces informations comme les informations directement et indirectement accessibles, soit : « *9° informations directement accessibles: les informations conservées dans les bases de données propres à un service répressif belge* ***ou dans des bases de données***

[17] Encore récemment, voir l'Avis n° 210/2026 du 2 octobre 2026 *concernant un avant-projet de loi relatif à l'interdiction administrative des personnes morales, des sociétés sans personnalité juridique, des associations ou groupements de fait constituant une menace grave et actuelle pour la sécurité nationale ; et un avant-projet de loi relatif aux recours devant le Conseil d'Etat contre les mesures d'interdiction administrative prévues par la loi du XXX relative à l'interdiction administrative des activités de certaines entités constituant une menace grave et actuelle pour la sécurité nationale (ADV-2026-00052)*, considérants nos 8-13.

[18] Voir la note de bas de page n° 16.

auxquelles ce service répressif a un accès direct par ou en vertu de la loi ou par ou en vertu des traités *internationaux liant la Belgique* [19]*; 10° informations* ***indirectement accessibles****: les informations qu'un service répressif belge* ***peut obtenir, sur la base d'une disposition de loi et sans*** *réquisition ni habilitation d'un magistrat,* ***d'autres autorités publiques ou de parties privées établies en Belgique***[20] » (mis en gras par l'Autorité)[21].

16. Le Projet implique par conséquent **d'autres responsables du traitement que les services répressifs, susceptibles de relever de la compétence de l'Autorité**, qui d'une manière ou d'une autre, sont tenus/libres de communiquer des données à caractère personnel aux services répressifs belges concernés, fût-ce par la simple mise à disposition de celles-ci en cas « *d'accès direct* »[22].

17. La **qualification d'une information disponible comme étant directement ou indirectement accessible** a un impact sur les délais applicables pour la communication des informations demandées[23] et partant également, sur le temps disponible pour évaluer l'éventuelle application d'un motif de refus le cas échéant lié à la protection des données. Dans ces conditions, **en ce qui concerne les informations qui sont traitées dans des banques de données qui ne relèvent pas de la responsabilité des services de police**, l'Autorité se demande **s'il ne conviendrait pas de définir/préciser dans le Projet ce qu'il est entendu par** « *bases de données auxquelles ce service répressif* ***a un accès direct*** » (mis en gras par l'Autorité). En effet, même dans le domaine policier, l'exposé des motifs indique que « *Les bases de données propres à la police intégrée sont, par exemple,*

---

[19] L'exposé des motifs précise ce qui suit :

« *Les informations* ***directement accessibles (9°)*** *sont les informations directement accessibles pour un service répressif belge donné. Par conséquent, les informations directement accessibles pour un service répressif belge (ex.: la police intégrée) ne le sont pas nécessairement pour un autre service répressif compétent (ex.: les services de recherche de l'Administration générale des Douanes et Accises). Les bases de données propres à la police intégrée sont, par exemple, les* ***banques de données telles que visées à l'article 44/2*** *de la loi sur la fonction de police, comme la* ***Banque de données nationale générale*** *(BNG). Certaines données de la BNG peuvent néanmoins être soumises à une limitation d'accès stricte via des marquages (codes). Dans ce cas, ces informations dites "douces" ne sont pas (plus) directement accessibles.*

Des exemples de bases de données auxquelles la police intégrée a accès par ou en vertu de la loi ou des traités internationaux liant la Belgique sont ***la Banque-Carrefour des véhicules*** *de la Direction pour l'immatriculation des véhicules du Service public fédéral Mobilité et* ***le registre national*** *du Service public fédéral Intérieur)* » (mis en gras par l'Autorité).

[20] L'exposé des motifs précise ce qui suit :

« *Les informations indirectement accessibles (10°) comprennent les informations qui sont stockées ou non dans des bases de données et pour lesquelles les services répressifs belges doivent introduire une demande auprès d'une autre autorité publique ou d'une partie privée établie en Belgique pour obtenir l'accès à celles-ci.*

L'obtention d'informations d'autres services publics ou de parties privées doit être explicitement autorisée sur la base d'une disposition légale (nationale ou internationale) ».

Plus loin, l'exposé des motifs donne l'illustration suivante :

« *La consultation par la police intégrée d'informations provenant des bases de données de l'Office des Étrangers (autre service public) ou la consultation des données d'enregistrement d'un hôtel (partie privée) sont des exemples dans lesquels les deux conditions liées aux informations indirectement accessibles sont réunies* ».

[21] Voir l'article 4, 8°, 9° et 10° du Projet.

[22] Quant à l'accès au Registre National, voir par exemple l'Avis n° 34/2024 du 15 avril 2024 *concernant une proposition de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour (CO-A-2024-139)*.

[23] Voir le considérant n° 7.

les banques de données telles que visées à l'article 44/2 de la loi sur la fonction de police, comme la Banque de données nationale générale (BNG). ***Certaines données de la BNG peuvent néanmoins être soumises à une limitation d'accès stricte via des marquages (codes)****. Dans ce cas, ces informations dites "douces"* ***ne sont pas (plus) directement accessibles*** » (mis en gras par l'Autorité). Autrement dit en théorie, que le service répressif ait **techniquement** un **accès direct *à la banque de données*** d'un autre responsable du traitement n'implique pas nécessairement qu'il aura **un accès direct *aux informations* recherchées**, sans que soit nécessaire l'intervention du responsable du traitement de cette banque de données.

18. Enfin, l'article 25, § 3, du Projet dispose que « *Le SPOC* ***a accès à toutes les informations dont disposent les autres services répressifs compétents belges****,* ***dans le respect des règles nationales applicables****, dans la mesure où cela est nécessaire à l'exécution des tâches qui lui incombent en vertu de la présente loi* » (mis en gras et souligné par l'Autorité). Le commentaire de l'article 25 explique que « *Afin de permettre une communication adéquate et rapide des informations, le SPOC* ***doit avoir accès aux informations disponibles pour les services répressifs belges. Il s'agit des informations directement et indirectement accessibles*** *telles que décrites (dans l'exposé des motifs relatif) à l'article 4, 9° et 10°, en tenant toujours compte des restrictions d'utilisation et des classifications d'application* » (mis en gras et souligné par l'Autorité).

19. S'il est très clair qu'aux fins de l'exécution de ses tâches en vertu du Projet, le SPOC doit pouvoir **traiter** les informations échangées, la manière dont il doit pouvoir **accéder** à celles-ci est moins claire. Deux situations se présentent.

20. Premièrement, le dispositif prévoit que le SPOC doit avoir accès aux informations **« dont disposent »** les autres services répressifs. Dans cette logique, l'article 15, 2., de la Directive (transposé dans l'article 26 du Projet) prévoit que « *Les États membres veillent à ce que leur point de contact unique soit composé de membres du personnel de leurs services répressifs compétents dont la participation est nécessaire à l'échange adéquat et rapide d'informations au titre de la présente directive* ». Autrement dit, les informations concernées doivent être traitées **dans les systèmes d'information des services répressifs**. Pour l'AGD&A et d'éventuels autres services répressifs (relevant de la compétence de l'Autorité) dans le futur, **il appartient au Demandeur de vérifier si un tel flux de données est déjà organisé en droit positif belge** (« *dans le respect des règles nationales applicables* » indique à juste titre l'article 25, § 3, du Projet) **et à défaut, de l'encadrer dans une norme de rang de loi**.

21. Deuxièmement, se pose la question de l'accès aux données « **disponibles** » aux services répressifs concernés mais qui ne sont pas encore collectées par ceux-ci. A cet égard, s'il convenait de faire collecter sans mesure coercitive des données par l'AGD&A (ou dans le futur, par un autre service

répressif), l'Autorité est d'avis qu'il appartiendrait à l'AGD&A de collecter elle-même ces données dans un premier temps, pour les communiquer/rendre accessibles ensuite au SPOC en vue de l'accomplissement de la finalité poursuivie. Ce n'est pas le SPOC qui, en lieu et place de l'AGD&A, sera habilité à collecter lui-même des données disponibles par ailleurs conformément aux règles régissant l'action de l'AGD&A. **L'exposé des motifs doit être adapté sur ce point**.

II.3. Absence de « mesures coercitives » et autorisations judiciaires éventuellement nécessaires

22. L'article 3, § 4, 1°, du Projet prévoit que le Projet « ***n'impose aucune obligation*** *aux services répressifs belges : 1° d'obtenir des informations par des* ***mesures coercitives*** » (mis en gras par l'Autorité). En relation avec cette disposition, l'exposé des motifs explique que « *Par ailleurs, l'échange d'informations sur la base de la présente loi* ***n'est possible que si aucune habilitation ni réquisition de l'autorité judiciaire compétente n'est nécessaire pour la collecte de ces informations****. Ainsi, une* ***réquisition d'un juge d'instruction*** *est nécessaire pour des mesures coercitives telles qu'une* ***perquisition*** *ou des* ***écoutes téléphoniques****. Une* ***réquisition d'un magistrat de parquet*** *est, par exemple, nécessaire pour* ***retrouver un numéro de téléphone*** *secret ou* ***un bilan d'entreprise*** *non publié ou pour* ***vérifier si une personne réside*** *à une certaine adresse. Il s'agit d'exemples d'informations qui ne sont* ***pas (encore) disponibles*** *et pour lesquelles, par exemple, une décision d'enquête européenne (DEE) ou une commission rogatoire est requise conformément aux canaux respectifs de* ***coopération internationale entre autorités judiciaires*** » (mis en gras par l'Autorité).

23. Qu'en est-il néanmoins des hypothèses dans lesquelles un responsable du traitement est obligé de communiquer des informations à la police (par exemple, des images de vidéosurveillance en exécution de l'article 9 de la Loi du 21 mars 2007 *réglant l'installation et l'utilisation de caméras de surveillance*), mais qu'il refuse de communiquer ces images, par exemple s'il défend que la communication des informations sollicitées n'est pas obligatoire ou que celle-ci n'est pas conforme au droit applicable ?

24. L'Autorité est d'avis que l'expression « *mesures coercitives* » reprise de la Directive n'est pas claire et **qu'il appartient au législateur belge de préciser la portée de la limitation consacrée dans la Directive et le dispositif du Projet, à l'aune de la terminologie utilisée en droit belge** (et conformément à ce droit). L'Autorité se demande s'il ne peut y être procédé par renvoi au rôle du ministère public et du juge d'instruction dans le cadre des règles régissant la coopération internationale entre autorités judiciaires. Il appartient au Demandeur de choisir la formulation la plus adaptée.

25. Ceci est d'autant plus pertinent qu'il est question par ailleurs dans le Projet **d'autorisation judiciaire**. Ainsi conformément à **l'article 13 du Projet**, le SPOC doit refuser la communication des informations

concernées lorsque « *l'autorisation judiciaire a été refusée* ». Et une dérogation est logiquement applicable aux délais de réponse aux demandes d'informations lorsqu'une autorisation judiciaire est nécessaire. Or le Projet se limite à définir l'autorisation judiciaire comme l'autorisation de l'autorité judiciaire compétente **sans que puissent être identifiées les hypothèses concrètement visées**.

26. C'est **l'exposé des motifs** qui apporte des informations complémentaires à ce sujet. Il indique tout d'abord ce qui suit : « *On entend par autorisation judiciaire (6°) **l'autorisation du ministère public**, et non celle d'un juge d'instruction ou d'un juge du fond. **L'article 21bis, § 1, troisième paragraphe, du Code d'Instruction Criminelle (C.I.Cr.)** stipule en effet que, dans tous les cas sauf ceux des personnes directement intéressées par une enquête pénale, il appartient au ministère public de donner accès, "même pendant l'instruction". Dans les cas prévus par la présente loi où les services de police ont besoin d'une autorisation judiciaire, l'article 21bis, § 1, troisième alinéa, du C.I.Cr.*[24] *doit donc être appliqué et le service de police doit contacter le magistrat compétent du ministère public* » (mis en gras par l'Autorité).

27. Et il précise plus loin « *Il convient de faire la distinction entre une habilitation ou une réquisition de l'autorité judiciaire compétente **et une autorisation de l'autorité judiciaire compétente**, laquelle n'est ni une habilitation ni une réquisition, mais est **dans certains cas nécessaire pour communiquer des informations** à d'autres services de police belges, et donc également étrangers (**ex.: informations sous embargo ou données ANPR** datant de plus d'un mois, cf. article 19). **Ces informations sont, malgré la nécessité d'une intervention judiciaire, bel et bien à la disposition d'un service répressif belge** et relèvent donc du champ d'application de la présente loi* » (mis en gras et souligné par l'Autorité).

28. Le commentaire de l'article 19 du Projet indique encore que « *les services de police belges ont, **par exemple**, besoin de l'autorisation de l'autorité judiciaire compétente pour obtenir les informations*

---

[24] Selon cette disposition :

« *§ 1er. Sans préjudice des dispositions des lois particulières, de l'application des articles 28quinquies, § 2, 57, § 2, 61ter et 127, § 2, et de la procédure visée aux paragraphes 2 à 9, la personne directement intéressée peut, à tout moment, en fonction de l'état de la procédure, **demander au procureur du Roi ou au juge d'instruction qu'il lui donne accès au dossier ou d'en obtenir une copie**.*

Est considérée comme personne directement intéressée : l'inculpé, la personne à l'égard de laquelle l'action publique est engagée dans le cadre de l'instruction, la personne soupçonnée, la partie civilement responsable, la partie civile, celui qui a fait une déclaration de personne lésée, ainsi que ceux qui sont subrogés dans leurs droits ou les personnes qui les représentent en qualité de mandataire ad hoc, de curateur, d'administrateur provisoire, de tuteur ou de tuteur ad hoc.

Dans tous les autres cas, la décision sur l'autorisation de consulter le dossier ou d'en obtenir copie est prise par le ministère public, même pendant l'instruction.

Les expéditions et copies des actes d'instruction et de procédure des juridictions et des parquets militaires supprimés concernant des dossiers définitivement jugés ou sur lesquels il a été statué par l'auditeur militaire ou l'auditeur général au 31 décembre 2003, ne peuvent être délivrées que sur autorisation expresse du ou de l'un des magistrats du ministère public délégués à cette fin par le Collège des Procureurs généraux.

Le greffe de la cour d'appel de Bruxelles est chargé de la délivrance des expéditions et copies visées à l'alinéa 4 » (mis en gras par l'Autorité).

suivantes : - les informations ***frappées, à l'échelle nationale, d'une forme d'embargo tel que*** *visé à l'article 44/8 de la loi sur la fonction de police, à l'article 11 de la loi du 10 juillet 2006 relative à l'analyse de la menace ou à l'article 19 de la loi du 29 mars 2024 portant création de la banque de données commune "Terrorisme, Extrémisme, processus de Radicalisation" et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police; - les informations qui ne peuvent être obtenues par les services de police belges que moyennant l'autorisation préalable du magistrat compétent,* ***telles que*** *les données ANPR datant de plus d'un mois* » (mis en gras et souligné par l'Autorité).

29. L'Autorité est d'avis qu'il conviendrait de **préciser la définition du concept d'autorisation judiciaire reprise dans l'article 4, 6°, du Projet, afin que s'en dégage à tout le moins clairement et exhaustivement les catégories d'hypothèses visées** (informations sous embargo en raison d'une information ou d'une instruction judiciaire ; accès à un dossier répressif judiciaire ; données traitées par la police mais dont la communication nécessite une autorisation (cas des données relatives aux mineurs d'âge et de certaines données ANPR)). Ceci contribuerait également à distinguer les hypothèses dans lesquelles une simple autorisation du pouvoir judiciaire est requise, des autres hypothèses dans lesquelles l'intervention du pouvoir judiciaire peut être vue comme une « *mesure coercitive* ».

30. Toujours s'agissant des autorisations judiciaires, au considérant n° 32 de son Avis (qui porte sur l'avant-projet), le COC indique ce qui suit :

> « *Bien que ni la LFP ni ses travaux parlementaires n'expliquent ce que l'on entend (forme et conditions) par « l'autorisation » de « l'autorité judiciaire », on pourrait argumenter que ce terme vise également l'« accord » du parquet compétent dont il est question dans (l'exposé des motifs de) l'avant-projet (même si, comme nous le disions, il convient d'éviter d'utiliser cette notion). Cependant, il n'existe aucune certitude à ce sujet, ce qui pourrait constituer pour cet aspect également une source de confusion et d'insécurité juridique.*
>
> ***Dans l'état actuel du droit et de la LFP, l'autorisation ne s'assortit d'aucune condition de forme, ce qui doit être évité*** *ne serait-ce que pour des raisons d'administration de la preuve.* ***Le présent avant-projet et son exposé des motifs passent également cet aspect entièrement sous silence.*** *Il a pourtant été établi dans un rapport du COC du 27 mai 2025 – qui a été transmis aux auteurs de l'avant-projet – concernant la transmission de données à caractère personnel de mineurs d'âge à Europol par la police belge (e.a. aux points 21 et 22) que dans le cadre du respect de l'article 44/7, 2e alinéa de la LFP (à savoir*

l'obtention de l'autorisation du magistrat compétent qui est exigée par la loi pour l'enregistrement dans la BNG de données relatives à un mineur qui n'a pas 14 ans accomplis), (1) la police rencontre non seulement des difficultés à apporter à l'autorité de contrôle (et à la personne concernée) la preuve de cette autorisation, mais aussi que (2) cette autorisation – pour autant qu'elle ait été donnée – peut également l'avoir été sous les formes les plus diverses (verbalement, par le biais d'une apostille, sous forme de mention dans un procès-verbal, etc. …).

Le COC prie les auteurs de l'avant-projet de remédier à cette lacune en prévoyant dans la loi quelques conditions de forme, et en stipulant au moins que cette autorisation doive être donnée par écrit ou, lorsqu'elle a d'abord été donnée verbalement dans un cas d'urgence ou d'urgence opérationnelle, confirmée par écrit dans les meilleurs délais (et au plus tard dans les 3 jours ouvrables) selon un procédé uniforme et univoque. Cette règle minimale s'appliquerait alors tant à l'autorisation dans le cadre du présent avant-projet *qu'à celle dans le cadre de l'application de l'article 44/7, 2e alinéa de la LFP* » (mise en gras modifiée par l'Autorité).

31. L'Autorité rappelle que conformément à l'article 50, al. 2, de la LTD (et aux articles 4, 4., et 19 de la Directive 2016/680), chaque responsable du traitement doit être en mesure de démontrer que le traitement est effectué conformément à la LTD (à la Directive 2016/680). Ce qui vaut par conséquent également pour l'autorité judiciaire dont les traitements relèvent de la compétence d'avis (mais pas de contrôle comme rappelé précédemment) de l'Autorité. **L'Autorité partage la préoccupation exprimée par le COC et est d'avis que le Projet doit être adapté dans la logique du considérant n° 32 de l'Avis du COC.** Prévoir des conditions de forme à l'autorisation judiciaire délivrée dans le cadre de la mise en œuvre du Projet constitue une garantie appropriée en relation avec l'obligation d'*accountability* et de nature à contribuer à la sécurité juridique des traitements de données mis en œuvre au profit de l'ensemble des parties concernées.

II.4. Protection des données et motifs de refus des demandes d'informations

32. Concernant les motifs de refus de communications des informations sollicitées, ceux-ci sont **limitativement énumérés par la Directive[25] et l'article 13, § 1er, du Projet** qui est rédigé comme suit :

[25] Le considérant n° 20 de la Directive indique ce qui suit :

« *Dans des cas exceptionnels, il pourrait être objectivement justifié pour un État membre de refuser une demande d'informations soumise à son point de contact unique. Afin de garantir le bon fonctionnement du système créé par la présente directive dans le respect total de l'état de droit, il convient de définir ces cas de manière exhaustive et de les interpréter de manière restrictive.*

« *Le SPOC **ne peut refuser** de communiquer les informations demandées **que** dans la mesure où l'un des motifs suivants s'applique :*

1° le SPOC ou les autres services répressifs compétents belges ne disposent pas des informations demandées ;

2° la demande d'informations ne satisfait pas aux exigences énoncées à l'article 4 de la directive (UE) 2023/977 ;

3° l'autorisation judiciaire a été refusée ;

*4° les informations demandées constituent des **données à caractère personnel autres que celles relevant des catégories de données à caractère personnel visées à l'article 20, 2°** ;*

*5° les informations demandées **se sont révélées inexactes, incomplètes ou ne sont plus à jour et ne peuvent être communiquées conformément à l'article 32, § 2, de la loi du 30 juillet 2018** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;*

6° il existe des raisons objectives de penser que la communication des informations demandées :

a) serait contraire ou porterait atteinte aux intérêts essentiels de la sécurité nationale ;

b) compromettrait le bon déroulement d'une enquête en cours en matière pénale ou la sécurité d'une personne physique ;

*c) porterait indûment atteinte aux **intérêts importants protégés d'une personne morale** ;*

7° la demande concerne :

a) une infraction pénale punissable d'une peine de niveau 1 en vertu du droit belge ; ou

b) une affaire qui ne constitue pas une infraction pénale en vertu du droit belge;

Toutefois, les règles énoncées dans la présente directive mettent fortement l'accent sur les principes de nécessité et de proportionnalité, offrant ainsi des garanties contre toute utilisation abusive des demandes d'informations, y compris lorsqu'elle entraînerait des violations manifestes des droits fondamentaux. Pour faire preuve de leur diligence générale, les États membres devraient donc toujours vérifier la conformité des demandes qui leur sont soumises au titre de la présente directive avec les principes de nécessité et de proportionnalité et devraient refuser les demandes qu'ils jugent non conformes ».

8° les informations demandées ont été initialement obtenues d'un autre État membre ou d'un pays tiers, et l'État membre ou le pays tiers en question n'a pas consenti à la transmission des informations.

Le SPOC fait preuve de diligence raisonnable pour évaluer si la demande d'informations soumise satisfait aux exigences énoncées à l'article 4 de la directive (UE) 2023/977, ***notamment concernant la question de savoir s'il existe une violation manifeste des droits fondamentaux****.*

Tout refus de demande d'informations ***ne concerne que la partie des informations demandées à laquelle se rapportent les motifs énoncés*** *au premier alinéa et est, le cas échéant, sans préjudice de l'obligation de communiquer les autres parties des informations conformément à la présente loi* » (mis en gras par l'Autorité).

33. Cette disposition appelle les cinq commentaires suivants.

34. **<u>Premièrement</u>, la Directive et le Projet ne font pas du non-respect des règles de protection des données un motif de refus de la communication de celles-ci**. Il semblerait en conséquence que **l'obligation et les possibilités de vérification** de ce respect (avant échange de données) **par le SPOC et les services répressifs s'en retrouveraient limitées**. Concrètement par exemple, qu'en serait-il de la communication de données qui seraient conservées au-delà de leur durée de conservation légale (articles 28, 5°, et 30 de la LTD) ; qui plus largement ne seraient pas traitées licitement (article 28, 1°, de la LTD) pour un motif autre que ceux listés dans le Projet (par exemple, des données qui s'avèreraient être collectées de manière illégale) ; d'un ensemble de données à caractère personnel dans lequel ne seraient pas (ou pas correctement) distinguées les données fondées sur des faits des données fondées sur des appréciations personnelles (article 32, § 1er, de la LTD) ; de données liées à une personne physique en raison d'un profilage automatisé (par exemple, un traitement de données automatisé au terme duquel une personne, sur la base des informations disponibles, serait automatiquement considérée comme une menace potentielle – émeutier, extrémiste, contrefacteur, trafiquant de drogues, etc.) non conforme à l'article 35 de la LTD ? **Sauf à considérer que de telles données ne sont pas *légalement* <u>disponibles</u>**, aucun motif de refus ne semblerait textuellement applicable. L'Autorité, qui comprend que le Demandeur est lié par les termes de la Directive, est néanmoins d'avis que **l'exposé des motifs devrait aborder ce questionnement**.

35. En toutes hypothèses, **les règles de protection des données consacrées dans la Directive 2016/680 et le Titre 2 de la LTD s'appliquent concomitamment à la Directive et au Projet qui n'y dérogent pas**. Le considérant n° 23 de la Directive rappelle que « *Il est particulièrement*

important que la protection des données à caractère personnel, conformément au droit de l'Union, soit garantie dans le cadre de tous les échanges d'informations effectués au titre de la présente directive. À cette fin, tout traitement de données à caractère personnel par un point de contact unique ou un service répressif compétent au titre de la présente directive devrait être effectué ***dans le plein respect de la directive (UE) 2016/680 du Parlement européen et du Conseil*** » (mis en gras par l'Autorité).

36. **Deuxièmement**, dans le même sens que la position exprimée par le COC dans son Avis (considérant n° 33), l'Autorité considère que les termes « *ne peut… que* » de l'article 13 du Projet, ont pour objectif l'énumération limitative des motifs de refus. Autrement dit, **lorsqu'un motif de refus se rencontre en pratique, le SPOC doit refuser la communication des données concernées**. **Le dispositif du Projet doit être adapté en ce sens** (« *Le SPOC* ~~**ne**~~ *refuse de communiquer les informations demandées* ~~**que**~~ *dans la mesure où l'un des motifs suivants s'applique :* … »).

37. **Troisièmement**, comme le COC l'indique à l'alinéa 2 du considérant n° 37 de son Avis « […] *il serait pertinent de se demander pourquoi les motifs de refus du projet d'article 13 (par ex. il n'y a pas d'autorisation du magistrat, il s'agit d'autres données à caractère personnel que les catégories visées au projet d'article 20, 2°, etc. …) ne devraient plus s'appliquer lorsqu'il s'agit d'un échange direct entre services de police ou entre un service de police belge et un SPOC d'un autre État membre (notamment en cas d'urgence). Le COC ne voit pas de justification raisonnable à cette dérogation, et l'avant-projet ne fait en tout état de cause valoir aucun argument en ce sens* ».

38. L'Autorité ne voit également aucune justification et est par conséquent d'Avis que **le Projet doit être adapté sur ce point** : **les motifs de refus visés à l'article 13 doivent également être applicables aux hypothèses d'échanges directs entre services répressifs concernés ainsi qu'aux hypothèses dans lesquelles le SPOC d'un autre Etat membre sollicite les services répressifs belges**. Peut-être cette modification pourrait-elle être directement apportée dans l'article 13 du Projet, de la manière suivante : « *Le SPOC* ~~**ne**~~ **ou, dans les cas visés aux articles 14, § 3, et 16, le service répressif belge,** *refuse de communiquer les informations demandées* ~~**que**~~ *dans la mesure où l'un des motifs suivants s'applique :* … ».

39. **Quatrièmement**, un commentaire semblable vaut *mutatis mutandis* **dans les hypothèses d'échange d'initiative d'informations**. En vertu de l'article 17, § 1er, du Projet, le SPOC et les services répressifs belges « ***peuvent*** » « *communiquer, de leur propre initiative* » des informations disponibles « *lorsqu'il existe des raisons objectives de penser que ces informations pourraient présenter un intérêt pour* » les Etats membres concernés aux fins concernées, et ils le **doivent** lorsque sont

en cause des « **infractions pénales graves** »[26]. Dans ces derniers cas, l'obligation « *n'existe pas dès lors que les motifs visés à l'article 12, § 1er, **3°*** [(autorisation judiciaire refusée)] ***et 6°*** [(raisons objectives de penser que la communication compromettrait le bon déroulement d'une enquête pénale en cours ou la sécurité d'une personne physique ou porterait indûment atteinte aux intérêts importants protégés d'une personne morale)], *s'appliquent à ces informations* » (mis en gras par l'Autorité). **Tout d'abord, l'Autorité ne perçoit pas pour quelle raison les motifs de refus visés aux 4° et 5° de l'article 13 ne seraient pas applicables**. **Le Projet doit être adapté sur ce point**.

40. En outre, l'Autorité ne perçoit pas quelle est l'hypothèse concrètement visée par l'expression « *porterait indûment atteinte aux intérêts importants protégés d'une personne morale* »[27] et la raison pour laquelle une discrimination serait ici établie entre personnes morales et personnes physiques. **En quoi la communication licite à un autre service répressif européen** (données adéquates, pertinentes, à jour, etc., communiquées conformément aux principes de la Directive – fiabilité et confidentialité en particulier, dans le respect des droits propres des personnes morales le cas échéant applicables), **de données traitées licitement par un service répressif belge, serait-elle susceptible de porter « *indûment* » atteinte aux intérêts « *importants* » d'une personne morale ?** Et si une telle atteinte est possible **pourquoi serait-elle alors admise à l'égard de personnes physiques ?**

---

[26] L'article 4, 5°, du Projet et la Directive définissent le concept d'infraction pénale grave par référence à d'autres instruments juridiques. Sont ainsi par exemple concernés, en relation avec la législation applicable au mandat d'arrêt européen, s'ils sont punis d'une peine privative de liberté maximum d'au moins 3 ans : 1° participation à une organisation criminelle; 2° terrorisme; 3° traite des êtres humains; 4° exploitation sexuelle des enfants et pédopornographie; 5° trafic illicite de stupéfiants et de substances psychotropes; 6° trafic illicite d'armes, de munitions et d'explosifs; 7° corruption; 8° fraude, y compris la fraude portant atteinte aux intérêts financiers des Communautés européennes au sens de la Convention du 26 juillet 1995 relative à la protection des intérêts financiers des Communautés européennes; 9° blanchiment du produit du crime; 10° faux monnayage et contrefaçon de l'euro; 11° cybercriminalité; 12° crimes contre l'environnement, y compris le trafic illicite d'espèces animales menacées, et le trafic illicite d'espèces et d'essences végétales menacées; 13° aide à l'entrée et au séjour irréguliers;14° homicide volontaire, coups et blessures graves; 15° trafic illicite d'organes et de tissus humains; 16° enlèvement, séquestration et prise d'otage; 17° racisme et xénophobie; 18° vols organisés ou avec arme; 19° trafic illicite de biens culturels y compris antiquités et ouvres d'art; 20° escroquerie; 21° racket et extorsion de fonds; 22° contrefaçon et piratage de produits; 23° falsification de documents administratifs et trafic de faux; 24° falsification de moyens de paiement; 25° trafic illicite de substances hormonales et autres facteurs de croissance; 26° trafic illicite de matières nucléaires et radioactives; 27° trafic de véhicules volés; 28° viol; 29° incendie volontaire; 30° crimes relevant de la juridiction de la Cour pénale internationale; 31° détournement d'avions ou de navires; 32° sabotage.

En relation avec la réglementation applicable à Europol qui appuie et renforce l'action des autorités compétentes des États membres et leur collaboration mutuelle dans la prévention de la criminalité grave affectant deux ou plusieurs États membres, du terrorisme et des formes de criminalité qui portent atteinte à un intérêt commun qui fait l'objet d'une politique de l'Union, ainsi que dans la lutte contre ceux-ci, listées ci-après : terrorisme, criminalité organisée, trafic de stupéfiants, activités de blanchiment d'argent, criminalité liée aux matières nucléaires et radioactives, trafic de migrants, traite des êtres humains, criminalité liée au trafic de véhicules volés, meurtre et coups et blessures graves, trafic d'organes et de tissus humains, enlèvement, séquestration et prise d'otage, racisme et xénophobie, vol qualifié et vol aggravé, trafic de biens culturels, y compris les antiquités et les œuvres d'art, escroquerie et fraude, infractions portant atteinte aux intérêts financiers de l'Union, délits d'initiés et manipulation des marchés financiers, racket et extorsion de fonds, contrefaçon et piratage de produits, falsification de documents administratifs et trafic de faux, faux-monnayage et falsification de moyens de paiement, criminalité informatique, corruption, trafic d'armes, de munitions et d'explosifs, trafic d'espèces animales menacées, trafic d'espèces et d'essences végétales menacées, criminalité au détriment de l'environnement, y compris la pollution causée par les navires, trafic de substances hormonales et d'autres facteurs de croissance, abus sexuels et exploitation sexuelle, y compris matériel pédopornographique et sollicitation d'enfants à des fins sexuelles, génocides, crimes contre l'humanité et crimes de guerre, violation des mesures restrictives de l'Union.

[27] En quoi la communication licite à un autre service répressif européen (les données sont proportionnées, etc.), de données traitées licitement par un service répressif belge, et en outre conformément aux principes de la Directive (en particulier confidentialité et fiabilité) est-elle susceptible de porter « *indûment atteinte* » aux intérêts « *importants* » d'une personne morale ? Et si une telle atteinte est possible s'agissant des personnes physiques, pourquoi devrait-elle être autorisée ?

L'exposé des motifs devrait être approfondi à ce sujet. L'Autorité réserve son analyse à ce propos.

41. Ensuite, l'Autorité rappelle que le traitement ultérieur des données, conformément à l'article 29, § 1er, 2°, de la LTD, doit être nécessaire et proportionné au regard du droit applicable. Conformément au principe d'*accountability* consacré dans l'article 50, al. 2, de la LTD, le service répressif concerné (l'AGD&A) devra être en mesure de démontrer que les données concernées présentent bien un intérêt réel concret (soit, sont bien nécessaires) pour le service répressif destinataire aux finalités concernées.

42. **Cinquièmement**, l'Autorité est d'avis que **la référence à « *l'existence d'une violation manifeste des droits fondamentaux* » est cryptique**. L'exposé des motifs doit clarifier ce dont il est question (s'agit-il de prévoir un motif général de refus en cas de violation manifeste d'un droit fondamental ? – le/squel/s ?) et l'Autorité réserve son analyse à ce sujet. En tout état de cause, **ce passage du Projet ne peut être lu comme limitant le pouvoir d'appréciation** du SPOC/**du service répressif concerné concernant la mise en œuvre des motifs de refus liés aux règles de protection des données** : il ne peut s'agir de limiter son appréciation à des violations *manifestes*.

II.5. Exactitude et caractère à jour des données

43. En vertu de **l'article 6, 5°**, du Projet, le SPOC et les services répressifs belges « *veillent à ce que* » « *les données à caractère personnel échangées au titre de la présente loi qui s'avèrent inexactes, incomplètes ou plus à jour soient effacées ou rectifiées ou que leur traitement soit limité, selon le cas, et que tout destinataire en soit informé sans tarder* ». L'Autorité rappelle l'application concomitante de l'article 32 de la LTD et soulignent que les responsables du traitement doivent **garantir** que lorsque les données sont inexactes, incomplètes ou plus à jour, celles-ci soient effacées, rectifiées ou que leur traitement soit limité et que tout destinataire en soit informé sans tarder.

44. L'Autorité est d'avis que **le Projet devrait prévoir que les responsables du traitement sont tenus d'agir dès que possible et au plus tard dans un délai fixé par le Projet à partir du moment où ils ont connaissance du caractère inexact, incomplet ou non à jour, des données concernées**. Plutôt que de recourir à l'expression floue « *sans tarder* ». Une obligation renforcée de ce type se justifie, de l'avis de l'Autorité, pour les raisons suivantes.

45. Premièrement, le **champ d'application de la Directive est très large**. Notamment, il vise la prévention des infractions pénales en général, et la définition des informations concernées, calquée sur celle de la Directive (article 2, 4)), est logiquement large – bien que limitée à une longue liste de catégories de données liées à des catégories de personnes, consacrée dans l'Annexe 2, section B, du Règlement (UE) n° 2016/794 du Parlement européen et du Conseil du 11 mai 2016 *relatif à l'Agence*

de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI. L'exposé des motifs quant à lui indique que « *Dans le domaine de la police administrative, les informations (7°) concernent tout contenu pouvant mener à l'identification de personnes pour lesquelles il existe, sur la base de précédents, d'une observation ou d'une analyse de risque, un soupçon fondé qu'elles pourraient participer à des infractions pénales* ». Deuxièmement, la **fiabilité de l'information concernée** est une exigence au cœur de la Directive et du Projet tant sur les points de vue opérationnel que de la protection des données. Troisièmement, ces textes prévoient des **délais stricts applicables aux réponses** aux demandes d'information de telle sorte qu'il est naturel d'agir dans leur contexte normatif, avec célérité. L'article 25, § 1er, prévoit d'ailleurs que le SPOC accomplit ses tâches 24 heures sur 24 et 7 jours sur 7.

46. En outre, l'Autorité invite le Demandeur à envisager si, dans la situation dans laquelle les services répressifs belges se basent de manière décisive sur des informations communiquées par un autre service répressif européen afin d'exercer une compétence concrète à l'égard de personnes concernées, il ne conviendrait pas de prévoir une prise de contact avec cet autre service afin de s'assurer du caractère complet, exact et à jour des données concernées.

II.6. Responsabilités au regard des traitements de données

47. S'agissant des responsabilités au regard du traitement, l'article 21 du Projet dispose que :

> « *Les responsables du traitement pour les traitements des données à caractère personnel au titre de la présente loi, à l'exception des traitements effectués au titre de l'article 28, § 1, sont :*
> - *le ministre de l'Intérieur et le ministre de la Justice, chacun dans le cadre de ses compétences, pour les traitements effectués par les services de police ;*
> - *l'administrateur général de l'Administration générale des Douanes et Accises pour les traitements effectués par l'Administration générale des Douanes et Accises ;*
> - *l'autorité désignée par le Roi pour les traitements effectués par les services qu'Il désigne en exécution de l'article 4, 2°* ».

48. Pour ce qui concerne les entités relevant du champ d'application de la compétence de l'Autorité, celle-ci rappelle qu'elle considère en général qu'**une autorité publique est responsable du traitement de données à caractère personnel nécessaire à l'exécution d'une mission d'intérêt public ou à une obligation légale qui lui incombe**, et elle a régulièrement considéré qu'il convenait de

désigner dans une norme du rang de loi, le responsable du traitement[28]. En l'occurrence, en tant que **service répressif belge** désigné par le projet, le **« *les services de recherches de l'Administration générale des Douanes et Accises* »** (plutôt que l'administrateur général de l'AGD&A) ont des responsabilités à l'égard du traitement de données en exécution du Projet et **sont par conséquent un responsable du traitement**.

49. L'Autorité a ensuite déjà souligné précédemment que **le Projet ne pouvait pas habiliter le Roi à étendre son application à d'autres services répressifs** compte-tenu de l'impact d'une telle extension sur la détermination des éléments essentiels des traitements de données à caractère personnel nécessaires en vue de l'exécution du Projet.

50. Selon les hypothèses, le Projet semble attribuer des responsabilités **conjointes ou propres** aux SPOC et aux services répressifs. L'article 6, du Projet (concernant son 5°, voir le **considérant n° 43**) prévoit en effet que « *le SPOC **et** les autres services répressifs belges veillent à ce que* » (mis en gras par l'Autorité). Tandis que l'article 20 du Projet prévoit généralement que « *le SPOC **ou** les autres services répressifs belges veillent à ce que* » (mis en gras par l'Autorité), notamment, les données à caractère personnel soient exactes, complètes et à jour. Quand l'échange a lieu **exclusivement entre services répressifs**, il serait effectivement cohérent d'imputer la responsabilité au regard des traitements de données au service répressif belge concerné. Dans les cas où le SPOC intervient cependant, c'est à celui-ci qu'il incombera de décider de l'application ou non d'un motif de refus lié aux principes de protection des données. **L'Autorité est d'avis que le Projet doit être clarifié lorsque les responsabilités qu'il consacre sont propres à chaque entité (SPOC ou service répressif) mais que les deux entités interviennent dans l'échange de données**. Par exemple, il semblerait logique que ce soit l'AGD&A qui mette à disposition du SPOC les éléments nécessaires permettant d'apprécier le degré d'exactitude, d'exhaustivité et de fiabilité des données concernées, mais c'est celui-ci qui devra transmettre ces informations au service répressif d'un autre Etat membre. Se pose également la question de savoir dans cadre si le SPOC peut/doit adapter ces données selon sa propre appréciation, auquel cas il ne serait pas conforme aux principes de protection des données d'attribuer exclusivement une responsabilité à l'AGD&A. **Dès lors que la responsabilité de l'application d'un motif de refus incombe au SPOC lorsqu'il intervient, il est important que le Projet garantisse que l'AGD&A ou tout autre service répressif futur qui serait concerné puisse/doive utilement faire valoir son point de vue de responsable du traitement initial des données collectées à**

[28] Voir le considérant n° 12 de l'Avis n° 210/2026 du 2 octobre 2026 *concernant un avant-projet de loi relatif à l'interdiction administrative des personnes morales, des sociétés sans personnalité juridique, des associations ou groupements de fait constituant une menace grave et actuelle pour la sécurité nationale ; et un avant-projet de loi relatif aux recours devant le Conseil d'Etat contre les mesures d'interdiction administrative prévues par la loi du XXX relative à l'interdiction administrative des activités de certaines entités constituant une menace grave et actuelle pour la sécurité nationale (ADV-2026-00052)*, et les références y citées.

l'attention du SPOC. De telle sorte que ce dernier puisse se positionner en parfaite connaissance de cause.

PAR CES MOTIFS,
L'Autorité est d'avis que,

1. Elle est bien compétente pour se prononcer à l'égard du Projet, s'agissant des traitements de données mis en œuvre par l'AGD&A, les autorités judiciaires et différents responsables du traitement qui sont tenus de communiquer des données aux services répressifs visés par le Projet (**considérants nos 8-21**) – le présent Avis ne porte pas sur les traitements de données réalisés par les services de police ;

2. L'article 4, 2°, du Projet doit être adapté de manière telle que le Roi ne puisse en définir le champ d'application quant aux services répressifs belges concernés (**considérant n° 13**) ;

3. En ce qui concerne les informations qui sont traitées dans des banques de données qui ne relèvent pas de la responsabilité des services de police, il convient d'envisager de définir/préciser dans le Projet ce qu'il est entendu par « *bases de données auxquelles ce service répressif a un accès direct* » (**considérants nos 15-17**) ;

4. Il convient de vérifier si le droit applicable aux échanges de données entre les services pertinents de l'AGD&A et les services de police prévoient déjà un accès direct du SPOC et l'exposé des motifs doit être adapté concernant l'accès aux données qui ne sont pas encore collectées par les services pertinents de l'AGD&A (**considérants nos 18-21**) ;

5. L'expression « *mesures coercitives* » reprise de la Directive n'est pas claire et il appartient au législateur belge de préciser la portée de la limitation consacrée dans la Directive et le dispositif du Projet, à l'aune de la terminologie utilisée en droit belge (et conformément à ce droit) (**considérants nos 22-24**) ;

6. Le dispositif du Projet doit préciser le concept d'autorisation judiciaire à l'aune de l'exposé des motifs et y attacher des exigences minimales de forme (**considérants nos 25-31**) ;

7. Le Projet doit être adapté s'agissant de l'applicabilité des motifs de refus relatifs aux principes de protection des données (**considérants nos 32-42**) ;

8. Le Projet devrait prévoir que les responsables du traitement sont tenus d'agir dès que possible et au plus tard dans un délai fixé par le Projet à partir du moment où ils ont connaissance du caractère inexact, incomplet ou non à jour, des données concernées (**considérants nos 43-46**) ;

9. Le Projet doit être adapté s'agissant de la détermination des responsabilités au regard du traitement de données à caractère personnel (**considérants nos 47-50**).

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