ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA260030		05.09.2026

Objet : Avis relatif à l'avant-projet de loi relatif à la création du *National Travel Targeting Center* et au traitement des informations préalables sur les passagers (API) en vue d'améliorer le contrôle aux frontières et de lutter contre l'immigration illégale.

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (*M.B.* du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1er, 2e alinéa, l'article 71 et le Titre 7, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (ci-après 'la LPI').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED*').

Vu la loi du 25 décembre 2016 relative au traitement des données des passagers.

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 »* (le règlement général sur la protection des données ou 'le RGPD').

Vu la demande du ministre de la Sécurité et de l'Intérieur du 5.08.2026.

Vu le rapport de Monsieur Ronny Saelens, membre-conseiller a.i. de l'Organe de contrôle.

Émet, le 05.10.2026, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD') dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans la loi du

---

[1] 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 »* (règlement général sur la protection des données ou « RGPD »).

[2] Directive (UE) 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 dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).

[3] Article 4 §2, 4e alinéa de la LAPD.

[4] Article 71 §1er, 3e alinéa de la LPD.

[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.

15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

4. L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale *« sur les douanes et accises »* du 18 juillet 1977, telle que modifiée par la loi du 16 mai 2024 *« modifiant la loi du 25 décembre 2016 relative au traitement des données des passagers »*.

5. Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (*M.B.* du 8 août 2022), de la validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

6. L'Organe de contrôle est compétent pour rendre des avis sur les aspects ayant trait au traitement des informations et des données à caractère personnel et à la protection de la vie privée par le traitement de données à caractère personnel pour autant qu'il existe un rapport avec le fonctionnement opérationnel et non opérationnel des services de police et/ou avec le personnel de la police intégrée (ci-après 'la GPI[7]') et/ou pour autant que le projet de texte soumis pour avis ait un impact sur la gestion de l'information policière en général.

7. Par ailleurs, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi une autorité de contrôle qui est légalement chargée de contrôler la légalité, l'efficacité, l'efficience et l'économie de la gestion de l'information policière[8].

---

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[7] Geïntegreerde politie – Police Intégrée.
[8] Rapport d'activité 2021, www.organedecontrole.be, voir les points 3 et 52 et plus spécifiquement le point 71 : *« Il serait cependant faux de s'imaginer que le COC se préoccupe seulement de la protection des données ; il porte aussi énormément d'attention à tous les autres aspects opérationnels de la gestion de l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence. »* ; article 71 §1er de la LPD.

II. Objet de la demande et antécédents

8. La demande d'avis a trait à l'avant-projet de loi *« relatif à la création du National Travel Targeting Center (ci-après 'le NTTC') et au traitement des informations préalables sur les passagers (API) en vue d'améliorer le contrôle aux frontières et de lutter contre l'immigration illégale »* (ci-après 'l'avant-projet').

9. L'avant-projet prévoit que les informations préalables sur les passagers – aussi appelées 'données API' – que le *NTTC* reçoit des transporteurs aériens soient transmises notamment aux services de police (compétents), qui sont désignés en tant qu'*« autorité compétente »*, et fassent l'objet d'un traitement ultérieur dans le cadre du contrôle aux frontières tel que visé dans l'avant-projet.

10. Selon la note au Conseil des ministres du 10.07.2026, il a été décidé de ne plus transposer dans la loi PNR la Directive 2004/82/CE du Conseil du 29 avril 2004 *« concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers »* (la directive API), et donc le traitement des données API, afin d'éviter toute confusion concernant les finalités du traitement de données à caractère personnel relevant respectivement de la directive API, d'une part, et de la Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 *« relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière »* (la directive PNR), d'autre part.

11. En réalité, la raison de cette scission est double :

1) L'arrêt n° 131/2023 du 12 octobre 2023 de la Cour constitutionnelle, qui a annulé certains articles de la loi du 25 décembre 2016 *« relative au traitement des données des passagers »* (ci-après 'la loi PNR') mais a par contre maintenu l'article critiqué de la loi PNR dans l'interprétation que la Cour lui confère dans son arrêt.
Dans son arrêt interlocutoire n° 135/2019 du 17 octobre 2019, la Cour constitutionnelle avait en effet posé à la Cour de Justice de l'Union européenne dix questions préjudicielles qui, en bref, avaient trait à la compatibilité de la loi PNR de l'époque avec la Charte des droits fondamentaux de l'Union européenne. Pour résumer, l'arrêt C-817/19 du 21 juin 2022 de la Cour de Justice permettait de déduire que (le champ d'application et la portée de) certains articles de la directive API et de la directive PNR n'avaient pas été transposés de manière légalement conforme dans la loi PNR belge.

2) Le Règlement (UE) 2025/12 du Parlement européen et du Conseil du 19 décembre 2024 *« relatif à la collecte et au transfert des informations préalables sur les passagers en vue de renforcer et de faciliter les vérifications aux frontières extérieures, modifiant les règlements (UE) 2018/1726 et (UE)*

2019/817, et abrogeant la directive 2004/82/CE du Conseil ». En vertu de son article 46, ce Règlement 2025/12 s'applique à compter de la date correspondant à deux ans à compter de la date de mise en service du routeur, telle qu'elle est déterminée par la Commission conformément à l'article 34[9]. Cette date n'ayant pas encore été déterminée par la Commission, l'auteur de l'avant-projet estime nécessaire de transposer encore la directive API en attendant la pleine application du Règlement 2025/12[10].

12. Dans le présent avis, l'Organe de contrôle se bornera à aborder les traitements qui devront selon l'avant-projet être effectués par les services de police. Pour les traitements effectués par les autres entités prévues dans l'avant-projet, le COC renvoie à l'avis de l'Autorité de protection des données.

III. Analyse de la demande

A) Remarque générale : le champ d'application

13. Le projet d'article 2 de l'avant-projet est formulé comme suit :
« La présente loi transpose la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, dénommée ci-après « la directive API », et exécute certaines dispositions du règlement (UE) 2025/12 du Parlement européen et du Conseil du 19 décembre 2024 relatif à la collecte et au transfert des informations préalables sur les passagers en vue de renforcer et de faciliter les vérifications aux frontières extérieures, modifiant les règlements (UE) 2018/1726 et (UE) 2019/817, et abrogeant la directive 2004/82/CE du Conseil, dénommé ci-après « le règlement 2025/12 ». ».

14. Si on le lit conjointement avec le point 11 du présent avis, il découle du projet d'article 2 susmentionné que l'avant-projet a trait et se limite au traitement des données à caractère personnel en vue d'une **finalité du RGPD**, à savoir les contrôles aux frontières extérieures de l'Union européenne[11]. La présence, dans l'intitulé de l'avant-projet, des mots *« et de lutter contre l'immigration illégale »*, n'y change rien (voir plus loin).

15. Se pose alors d'emblée la question de la relation entre l'avant-projet et d'<u>autres</u> (projets de) cadres juridiques attribuant également à la police une <u>mission dans le cadre du contrôle aux frontières</u> qui relève d'une finalité du RGPD. Le COC renvoie à ce sujet à son avis (négatif) DA260028 du 15.09.2026 relatif à un projet d'arrêté royal *« modifiant l'arrêté royal du 8 octobre 1981 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, en ce*

[9] Une infrastructure centrale qui collectera toutes les données des passagers (données API et données PNR) reçues des transporteurs aériens et les transférera aux autorités compétentes de chaque État membre (article 11 du Règlement 2025/12).
[10] Exposé des motifs de l'avant-projet.
[11] À noter que la Directive 2004/82/CE du Conseil du 29 avril 2004 est encore mise en relation avec la Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, laquelle a été abrogée par le RGPD. Selon l'article 3.2 de cette Directive 95/46/CE, celle-ci ne s'appliquait pas aux traitements effectués dans le cadre notamment de la sécurité publique et du droit pénal.

qui concerne la mise en œuvre du Pacte européen sur l'asile et la migration » (www.organedecontrole.be) ainsi qu'aux références qui sont faites dans l'avis susmentionné aux remarques formulées dans d'autres avis et en particulier dans l'avis DA250026 du 6 février 2026 relatif à l'avant-projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers en vue de la mise en œuvre du Pacte sur la migration et l'asile de l'Union européenne[12]. L'auteur de l'avant-projet est donc prié de bien vouloir examiner ce point et de remédier le cas échéant aux éventuelles incohérences entre les différents projets de loi et/ou arrêtés d'exécution.

B) La compétence de la police à la lumière du champ d'application de l'avant-projet

16. Selon son article 6, l'avant-projet s'applique uniquement aux données API qui sont traitées par les transporteurs aériens et qui, dans le cadre de la finalité de l'avant-projet, sont transférées par l'intermédiaire du *NTTC* à l'*« autorité compétente »* (cf. projet d'article 11 de l'avant-projet). Selon le projet d'article 3 (ce numéro est manquant dans la version néerlandaise), 3° de l'avant-projet, *« les services de police chargés du contrôle des frontières »* sont désignés en tant qu''autorité compétente'.

17.1. Pour commencer, le COC se demande si l'auteur de l'avant-projet vise un certain service de police tel que visé à l'article 2, 2° de la LPI. La police intégrée a en effet été organisée à deux niveaux : la police *fédérale* et les corps de police *locale*. Si l'auteur de l'avant-projet vise en réalité uniquement la police fédérale, il serait préférable de l'indiquer explicitement dans l'avant-projet. Dans le cas contraire, il convient de préciser si – et, dans l'affirmative, pourquoi – la police locale a également un rôle à jouer en la matière, et le cas échéant de quel rôle il s'agit concrètement.

17.2. Deuxièmement, il est en l'occurrence attribué au service de police (désigné dans l'avant-projet) **une mission autre que les missions de police administrative et judiciaire** visées au Titre 2 de la LPD et dans la LFP. Le projet d'article 14 de l'avant-projet le confirme d'ailleurs explicitement en stipulant que les traitements de données effectués par l'*« autorité compétente »* (en l'occurrence la police) **relèvent du champ d'application du RGPD**.

17.3. Bien que l'avant-projet ne prétende nullement le contraire, nous faisons remarquer par souci de clarté qu'il n'est pas exclu que les services de police qui sont désignés à l'article 26, 7°, a) du Titre 2 de la LPD en tant qu'*« autorité compétente »* se voient **également** attribuer des missions relevant du RGPD. Dans ce dernier cas, cependant, le service de police visé dans l'avant-projet, qui est chargé du contrôle aux frontières, ne peut **pas** être considéré comme une *« autorité compétente »* au sens de l'article 26, 7°, a) du Titre 2 de la LPD (tout comme pour les traitements relevant du RGPD que les services de police effectuent dans le cadre d'autres missions – non policières –, comme la gestion du

[12] Avis disponible sur le site www.organedecontrole.be/publications/avis-r%C3%A9glementation.

personnel et la gestion financière et/ou logistique)[13]. En ce sens, le COC peut comprendre que l'auteur de l'avant-projet veuille prévoir cette mission relevant du RGPD dans une loi distincte, d'autant que cela a également un impact sur le traitement des données API par le service de police désigné et sur les droits de la personne concernée (voir plus loin).

Pour toute clarté, le traitement des données à caractère personnel dans le cadre de la finalité de l'avant-projet ne constitue donc **pas** une application d'un traitement tel que visé à l'article 29 de la LPD, lequel a trait par essence à la compatibilité du traitement ultérieur des données à caractère personnel à des fins autres que celles prévues au Titre 2 de la LPD, et donc aussi dans la LFP.

C) La responsabilité du traitement des données à caractère personnel

18. Selon le projet d'article 4 de l'avant-projet, il est prévu d'instituer au sein du Centre de crise national le *NTTC*, *« qui assure la gestion et la coordination des missions »* qui sont attribuées à l'Unité d'information des passagers (BELPIU) et à l'Unité nationale ETIAS (E.N.E.).

19. Dans ce contexte, le *NTTC* ferait, comme le prévoient les projets d'articles 5 et 8, office de *« point central de réception des données des passagers »*, telles que définies à l'article 4, 17° de la loi PNR, après quoi les données API reçues de la part des transporteurs aériens sont, selon le projet d'article 11, transmises par le *NTTC* à l'entité de police chargée du contrôle des frontières (l'autorité compétente).

20. Se pose alors la question de savoir qui est au sens de l'article 4, 7) du RGPD le responsable du traitement pour les différents traitements, à savoir pour (1) la transmission de ces données au service de police désigné et (2) la réception et l'utilisation de ces données par ce service de police désigné.

21. Le projet d'article 15 §2 de l'avant-projet désigne le service de police (l''autorité compétente') en tant que responsable du traitement pour les données API qui sont reçues de la part du *NTTC*. Et il va de soi que ce même service de police est également responsable de l'utilisation de ces données dans le cadre du contrôle des frontières. Dans l'intérêt de la sécurité juridique, il est indiqué de reprendre dans le projet d'article 3 de l'avant-projet, sous un numéro distinct, la notion de *« responsable du traitement »* en renvoyant à la définition qui en est donnée dans le RGPD.

D) Le traitement de données

22. Le projet d'article 12 de l'avant-projet est formulé comme suit (*verbatim*) :

[13] Cf. CJUE 21 juin 2022, C-817/19, points 66-68, faisant référence à une jurisprudence antérieure. Bien qu'il soit dans la jurisprudence évoquée question de 'particuliers' (sous la forme d'entreprises), il convient de faire remarquer que le RGPD s'applique également aux autorités, services et organismes publics, dont font donc également partie, au sens du RGPD, les services de police lorsqu'ils traitent des données à caractère personnel en vue de finalités du RGPD.

« L'autorité compétente traite les données reçues uniquement aux fins d'améliorer l'efficacité des vérifications aux frontières et de lutter contre l'immigration illégale, conformément à l'article 7 du règlement 2025/12 et à l'article 8, paragraphe 2 sexies et paragraphe 3, point i bis), du règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen). ».

23. En ce qui concerne la limitation de la finalité telle qu'elle est prévue au projet d'article 12 de l'avant-projet, les points *« sexies »* et *« i bis) »* de l'article 8 du Règlement 2016/399 auxquels l'avant-projet fait référence ne semblent pas figurer dans ledit Règlement (actuelle version coordonnée du 12.10.2025), de sorte que ces références sont en ce sens erronées. Il revient à l'auteur de l'avant-projet de vérifier ce point.

24. Le projet d'article 13 de l'avant-projet est formulé comme suit (*verbatim*) :

« L'autorité compétente conserve les données reçues dans un fichier temporaire et les efface après vingt-quatre heures, à moins qu'elles ne soient nécessaires ultérieurement dans le cadre du contrôle des frontières. Dans cette hypothèse, les données sont effacées au maximum 48 heures après leur transmission par le NTTC. ».

En ce qui concerne la prévisibilité de la norme légale

25. D'un point de vue juridique, le projet d'article 13 ne semble pas être conforme au principe de limitation de la finalité tel qu'il est prévu au projet d'article 12 de l'avant-projet en ce sens que la première partie de la 1re phrase du projet d'article 13 (*« L'autorité compétente conserve les données reçues dans un fichier temporaire et les efface après vingt-quatre heures »)* semble viser (également) une finalité différente (?) ou plus vaste (?) que la finalité poursuivie par l'avant-projet, puisque seule la deuxième partie de la 1re phrase (*« à moins qu'elles ne soient nécessaires ultérieurement dans le cadre du contrôle des frontières »*) semble se rapporter au champ d'application de l'avant-projet – sauf si l'auteur de l'avant-projet vise dans la première partie de la phrase une autre finalité **dans le cadre du contrôle des frontières**.

26. En outre, le terme *« hypothèse »* est également inconciliable avec le principe de légalité, qui stipule que la norme légale, pour qu'elle soit prévisible pour le sujet de droit, doit être suffisamment claire et précise en fonction du traitement visé. Or, partant de la formulation de cette deuxième phrase, les traitements et conditions visés semblent pouvoir être *hypothétiques* et il y aurait également encore d'autres 'hypothèses' que la finalité du 'contrôle des frontières', ce qui ne devrait pas être possible.

27. Il appartient à l'auteur de l'avant-projet de clarifier les éléments soulevés dans les remarques formulées aux points 25 et 26.

La conservation et l'effacement des données et/ou du fichier

28. Selon le projet d'article 13 susmentionné de l'avant-projet, les *« données reçues* [sont conservées] *dans un fichier temporaire »* (soulignement du COC). Quelques remarques s'imposent à cet égard.

29.1. Pour commencer, la portée du projet d'article semble se limiter aux données *reçues* (et en particulier à leur conservation et à leur effacement). Il n'est donc pas possible de déterminer clairement si cette disposition vise exclusivement les données à caractère personnel (données API) qui sont reçues de la part du *NTTC*, comme le prévoit le projet d'article 11 lu conjointement avec le projet d'article 12 de l'avant-projet, ou si elle pourrait viser aussi d'autres données à caractère personnel qui auraient par exemple été consultées par l'entité de police chargée du contrôle des frontières et dont la conservation serait nécessaire dans le cadre de la finalité prévue au projet d'article 12.

29.2. Deuxièmement, la formulation *« données reçues dans un fichier temporaire »* prête à confusion. Le mot *« temporaire »* se rapporte-t-il aux *données* ou au *fichier* ? Et s'agit-il d'un seul fichier dans lequel sont conservées toutes les données reçues de la part du *NTTC*, ou bien de fichiers individuels ?

29.3. Et enfin, est-il procédé uniquement à l'effacement des données dans le fichier, ou aussi à l'effacement du 'fichier' en tant que tel, qui constitue le support des données ?

30. Selon la formulation du point 2 de l'article 8 du Règlement 2025/12, il apparaît toutefois que la conservation et l'effacement ont trait aux données API. En outre, l'article susmentionné ne fait pas non plus mention d'un support donné (le 'fichier') dans lequel les données API seraient conservées. Nous revenons sur ce dernier point dans la troisième remarque qui suit.

31. Une troisième remarque a en effet trait au terme *« fichier »* figurant au projet d'article 13 de l'avant-projet. Il n'est en effet pas exclu que le législateur national réglemente le support dans lequel les données sont traitées (conservées). Dans l'optique du droit de la protection des données, l'auteur semble toutefois vouloir désigner par le terme *« fichier »* (qui a été traduit par *« dossier »* dans la version néerlandaise) la notion de *« fichier »* telle que visée à l'article 4, 6) du RGPD, comme l'enregistrement de données à caractère personnel dans des dossiers *manuels*[14]. Le RGPD établit en effet une distinction entre un traitement *« automatisé »* (en tout ou en partie) et le traitement (non automatisé) de données à caractère personnel contenues ou appelées à figurer dans un *« fichier »*

[14] Voir aussi, fût-ce dans un autre contexte, CJUE 10 juillet 2018, témoins de Jehova, C-25/17.

(article 2.1. AVG). Cela dit, il n'est évidemment pas exclu qu'il soit prévu que les deux formes de traitements puissent avoir lieu. L'une forme de traitement n'exclut en effet pas l'autre.

La question qui se pose est de savoir si l'auteur de l'avant-projet a vraiment l'intention de laisser les services de police travailler avec un fichier sur papier, voire de les y obliger.

32. Sans préjudice des remarques formulées aux points 25 et 26, le COC recommande donc d'amender comme suit la première partie de la 1re phrase du projet d'article 13 de l'avant-projet :

« L'autorité compétente ne conserve pas les données plus de vingt-quatre heures, (…) ».

Cette formulation correspond aussi (mieux) à l'objectif de l'article 8.2 susmentionné du Règlement 2025/12, dont le projet d'article 13 de l'avant-projet semble être la transposition.

33. Par souci de clarté, il convient ici de faire remarquer qu'en ce qui concerne le traitement des données API dans une *banque de données*, l'exposé des motifs renvoie à l'arrêt n° 131/2023 du 12 octobre 2023 de la Cour constitutionnelle, qui stipule par essence au point B.54.2 que les données poursuivant une finalité relevant du RGPD ne peuvent pas être traitées dans la même banque de données que celle créée pour les données PNR (c'est-à-dire des données poursuivant des finalités relevant du Titre 2 de la LPD). Le COC comprend l'objectif de cette considération de droit de la Cour constitutionnelle et la raison pour laquelle l'auteur de l'avant-projet y fait référence, en ce sens que les données à caractère personnel ne peuvent pas, lorsqu'elles sont traitées en vue du champ d'application de l'avant-projet, l'être dans les banques de données policières opérationnelles telles que visées à l'article 44/2 §2 de la LFP. Il en découle que les données à caractère personnel visées au projet d'article 13 susmentionné de l'avant-projet ne peuvent en principe être traitées ni dans la Banque de données nationale générale, ni dans une banque de données de base, ni dans une banque de données particulière. Elles devront donc l'être dans une autre banque de données ou un autre fichier que les banques de données policières existantes telles que prévues dans la LFP.

34. Il découle de ce qui précède que le service de police chargé du contrôle des frontières devra respecter les obligations du RGPD, et notamment prendre les mesures techniques et organisationnelles appropriées dans le cadre de la protection des données à caractère personnel. L'une des mesures qui en font partie est celle qui consiste à déterminer les droits d'accès, telle qu'elle est prévue au projet d'article 12, 2e alinéa de l'avant-projet. Le COC ignore si les services de police, et en particulier la police fédérale, en sont bien informés et savent donc aussi qu'il leur faudra procéder aux adaptations et/ou investissements requis sur le plan des technologies de l'information. Comme le ministre qui a sollicité l'avis est également le ministre de tutelle de la police fédérale, on peut supposer que cela aura effectivement été le cas.

35. Cela signifie toutefois aussi que les personnes concernées auront le droit de demander à pouvoir accéder aux données à caractère personnel les concernant qui sont traitées par le service de police chargé du contrôle des frontières et ce, pour toute clarté, **au moyen d'un système d'accès direct auprès du service de police responsable du traitement** (et donc **pas** par l'intermédiaire du COC dans le cadre du système d'accès indirect prévu en vertu du Titre 2, et plus précisément des articles 41 et 42, de la LPD, tel qu'il existe toujours à l'heure actuelle[15]).
Afin de ne faire naître aucun doute sur ce point, l'auteur de l'avant-projet est prié de prévoir et de détailler ce point dans l'avant-projet.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le demandeur de tenir compte des remarques susmentionnées.

Avis approuvé par l'Organe de contrôle de l'information policière le 05.10.2026.

Pour l'Organe de contrôle,
Le président *a.i.,*
Frank SCHUERMANS (Sé)

[15] Nous ne nous attarderons pas ici sur le constat que ce système d'accès indirect systématique par l'intermédiaire du COC, qui existe depuis 2018 et qui est unique au sein de l'UE, n'est pas compatible avec le droit européen en vigueur. Ce point est exposé en détail dans le dernier rapport d'activité du COC (2025), avec des références aux verdicts rendus à ce sujet par la Cour de Justice de l'Union européenne et la Cour d'appel de Bruxelles. Le rapport d'activité 2025 est disponible sur le site www.organedecontrole.be/publications/rapports-annuels.