



ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA220016		4.07.2022

Objet : Avis relatif à un 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 ce qui concerne le système d'entrée/de sortie

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 §1, 2^e al, 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 'LCA').

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

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 la demande d'avis, reçue sur support électronique par l'Organe de contrôle le 6 mai 2022, d'émettre un avis conformément à la LPD susmentionnée.

Vu le rapport de Monsieur Koen Gorissen, membre-conseiller de l'Organe de contrôle.

Émet, le 4 juillet 2022 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 2016/679¹ et de la Directive 2016/680², le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi organique du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après dénommée en abrégé 'LAPD') dispose qu'à l'égard des services de police au sens de l'article 2, 2^o, 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 les services de police traitent des données à caractère personnel en dehors du cadre des missions de police administrative et judiciaire, par exemple en vue 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 §1^{er}, 2^e 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 1^{er} (pour les traitements non opérationnels)³ et du Titre 2 (pour les traitements opérationnels) de la LPD⁴. Le COC est en outre investi aussi d'une mission d'avis d'office, prévue à l'article 236 §2 de la LPD, et d'une mission de sensibilisation du public, des personnes concernées, des responsables du traitement et des sous-traitants à la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

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 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 police⁵.

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'), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après

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, 4^e alinéa de la LPD.

⁴ Article 71 §1^{er}, 3^e alinéa de la LPD.

⁵ Articles 59 §1^{er}, 2^e alinéa et 236, §2 de la LPD.

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 lois⁶.

4. Enfin, 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 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers.

II. Objet de la demande

5. La demande concerne un 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 ce qui concerne le système d'entrée/de sortie (ci-après 'l'avant-projet de loi').

6. Le secrétaire d'Etat pour l'asile et la migration a adressé le 6 mai 2022 une demande à l'Organe de contrôle afin que celui-ci émette un avis sur le projet de loi.

7. Les autorités ainsi que les traitements de données à caractère personnel et informations tombant exclusivement sous la compétence du COC sont strictement définis par la loi. L'Organe de contrôle limite par conséquent ses avis aux traitements qui tombent sous sa compétence, c'est-à-dire en l'espèce ceux qui sont effectués par les services de police ou qui ont un effet sur le travail des services de police.

En tous les cas, les avis du COC ne se limitent pas nécessairement à l'article ou aux articles indiqué(s) dans une demande d'avis. En effet, le COC tient toujours compte de tous les éléments et dispositions qui relèvent de sa compétence en vertu de la réglementation susmentionnée.

L'Organe de contrôle n'est pas seulement une autorité de protection des données mais est aussi chargé du contrôle et de la surveillance des banques de données policières⁷ et de tous les traitements policiers, aussi en termes de légalité, d'efficacité et d'effectivité. Ces éléments (p. ex. la faisabilité et les capacités opérationnelles) sont également pris en considération dans chaque demande d'avis.

III. Analyse de la demande

8. La demande d'avis requiert que l'avis soit remis selon la procédure d'urgence.

⁶ Article 71, §1^{er}, troisième alinéa juncto article 236, §3 de la LPD.

⁷ Voyez le rapport d'activités 2020 du COC, https://www.organedecontrôle.be/files/Rapport-d'activité_COC_2020_F.pdf, paragraphes 7 et 8.

L'Organe de contrôle rappelle que comme l'a déjà souligné l'Autorité de protection des données, la procédure d'urgence est réservée *« aux cas où l'urgence est étrangère au fait du demandeur, à savoir ceux où il eut été impossible de consulter l'Autorité plus tôt. Il en va notamment ainsi lorsque la norme est liée à une situation imprévisible »*⁸.

Les éléments apportés par le demandeur afin de justifier la demande urgente ne répondent pas à ces conditions. En effet, même si l'entrée en application du Règlement relatif à l'Entry Exit System (EES) ('Règlement 2017/2226' ou 'Règlement EES') a récemment été fixée à fin 2022, il s'agit d'un Règlement datant du 30 novembre 2017, entré en vigueur depuis **fin 2017**. En outre, l'article 38 du Règlement EES, relatif aux responsabilités incombant aux Etats membres telles que par exemple l'intégration de l'infrastructure frontalière nationale existante et de sa connexion à l'IUN⁹, l'organisation des points d'accès centraux et de leur connexion à l'IUN à des fins répressives, ou encore la gestion et des modalités de l'accès à l'EES du personnel dûment autorisé et du personnel dûment habilité des autorités nationales compétentes, est entré en vigueur depuis le **29 décembre 2017**.

La demande d'avis a par conséquent été traitée selon la procédure normale.

9. Au vu du projet de grande ampleur *« smart borders package »*¹⁰ en cours, de la prochaine entrée en application du nouveau cadre SIS¹¹, de la prochaine mise en œuvre des règlements relatifs à l'interopérabilité¹² et du système ETIAS¹³, ainsi que de leurs conséquences et implications juridiques et techniques au niveau national, et en ayant égard

⁸ Autorité de protection des données, *Avis concernant un avant-projet de décret relatif à la lutte contre le dopage et sa prévention*, (CO-A-2021-033), n° 26/2021 du 12 mars 2021, points 11 et 12.

⁹ Interface Uniforme Nationale.

¹⁰ Ce paquet législatif vise à mettre en place une gestion moderne, efficace et efficiente des frontières extérieures trouvant un équilibre entre la facilitation pour les voyageurs et la sécurité intérieure (voyez https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders_fr, consulté le 22 juin 2022), et la construction d'une architecture de gestion des données plus robuste et plus intelligente (voyez Communication de la Commission au Parlement européen et au Conseil, *Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité*, 6 avril 2016, <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52016DC0205>, consulté le 20 juin 2022).

¹¹ Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission ; Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 ; Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier.

¹² Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil et Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816.

¹³ Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) no 1077/2011, (UE) no 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226.

aux différentes demandes d'avis qu'il a reçues ces trois derniers mois¹⁴, l'Organe de contrôle se demande, de manière plus générale, si un travail de révision et de mise en conformité davantage intégré au niveau national n'aurait pas été plus opportun.

10. Pour le présent avis, l'Organe de contrôle comprend sous "traitements (de données et d'informations) dans le cadre de l'EES" l'introduction, la modification, l'effacement et la consultation de données visées aux articles 14, 16 à 20 du Règlement EES pour les finalités visées aux articles 23 à 35 du même règlement, ainsi que les éventuels traitements de ces données et informations dans des fichiers nationaux, pour les mêmes finalités.

11. L'*Entry Exit System* (EES) est composé¹⁵ :

- d'un système central ;
- d'une interface uniforme nationale (IUN) dans chaque Etat membre ;
- d'un canal de communication sécurisé entre l'EES et le système central du VIS¹⁶ ;
- d'une infrastructure de communication sécurisée et cryptée entre le système central de l'EES et les IUN ;
- d'un service internet ainsi que d'un répertoire de données.

12. L'EES doit permettre de s'assurer du respect des dispositions relatives à la période de séjour autorisé sur le territoire des Etats membres. A cette fin, l'EES permet d'enregistrer la date, l'heure et le lieu d'entrée et de sortie des ressortissants de pays tiers admis pour un court séjour sur le territoire des Etats membres et de calculer la durée de séjour autorisé¹⁷.

L'EES est également destiné à produire des signalements à l'intention des Etats membres lorsque le séjour autorisé a expiré, ainsi que d'enregistrer le moment et le lieu du refus d'entrée opposé aux ressortissants de pays tiers auxquels l'entrée pour un court séjour a été refusée¹⁸.

13. Les traitements de données à caractère personnel exécutés dans le cadre du EES doivent être conformes aux dispositions du RGPD et/ou de la Directive police-justice¹⁹, *in concreto* au Titre 2 LPD et à la LFP en particulier pour ce qui concerne les services de police.

¹⁴ Outre la présente demande d'avis, notamment : une demande d'avis relatif à un avant-projet de loi relatif au fonctionnement et à l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, dans le domaine des vérifications aux frontières et aux fins du retour des ressortissants de pays tiers en séjour irrégulier (référence COC, DA220017) ; une demande d'avis relatif à l'adaptation de la fiche C22 non publiée relative aux signalements internationaux de la Directive commune MFO-3 du 14 juin 2002 des Ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative (référence COC, DA220018) ; une demande d'avis relatif à un avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur (référence COC, DA220021).

¹⁵ Article 7 du Règlement EES.

¹⁶ Règlement (CE) 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les Etats membres sur les visas de court séjour (règlement VIS).

¹⁷ Considérant 7 du Règlement EES.

¹⁸ Article 1^{er} du Règlement EES.

¹⁹ Articles 49 et 58 du Règlement EES.

14. L'Organe de contrôle rappelle que, en vertu de l'article 22 de la Constitution, chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

Sur ce point, la Cour constitutionnelle a d'ailleurs récemment rappelé dans un arrêt du 10 mars 2022²⁰ que *"les éléments essentiels des traitements de données à caractère personnel doivent être fixés dans la loi elle-même. À cet égard, quelle que soit la matière concernée, constituent, en principe, des éléments essentiels, les éléments suivants :*

1°) les catégories de données traitées ;

2°) les catégories de personnes concernées ;

3°) la finalité poursuivie par le traitement ;

4°) les catégories de personnes ayant accès aux données traitées et ;

5°) le délai maximal de conservation des données (avis de l'assemblée générale de la section de législation du Conseil d'État n° 68.936/AG du 7 avril 2021 sur un avant-projet de loi « relative aux mesures de police administrative lors d'une situation d'urgence épidémique », Doc. parl., Chambre, 2020-2021, DOC 55-1951/001, p. 119). » (considérant B.13.1)."

Une délégation par la loi à un autre pouvoir est possible *"pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur"* (considérant B.13.1).

Outre l'exigence de légalité formelle, l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme et avec les articles 7, 8 et 52 de la Charte, impose que l'ingérence dans l'exercice du droit au respect de la vie privée et du droit à la protection des données à caractère personnel soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence (B.13.2).

Le niveau requis de précision de la législation concernée – laquelle ne peut du reste parer à toute éventualité – dépend notamment du domaine qu'elle est censée couvrir et du nombre et de la qualité de ses destinataires (CEDH, grande chambre, 4 décembre 2008, S. et Marper c. Royaume-Uni, §§ 95 et 96). Ainsi, la Cour européenne des droits de l'homme a jugé que l'exigence de prévisibilité dans des domaines liés à la sécurité nationale ne pouvait avoir la même portée que dans d'autres domaines (CEDH, 26 mars 1987, Leander c. Suède, § 51; 4 juillet 2006, Lupsa c. Roumanie, § 33) (B.13.2).

15. Une fois entré en application, le Règlement EES sera d'application directe en droit belge.

Dans les cas où ce Règlement laisse une marge de manœuvre aux Etats membres ou s'il est renvoyé spécifiquement au droit national, les éléments essentiels des traitements concernés doivent se retrouver

²⁰ Cour constitutionnelle, arrêt n° 33/2022 du 10 mars 2022, www.courconstitutionnelle.be.

dans la loi belge en des termes clairs et suffisamment précis, tenant évidemment compte de la sensibilité de la matière concernée.

16. L'avant-projet de loi faisant l'objet du présent avis a pour ambition de partiellement exécuter le Règlement 2017/2225²¹ et le Règlement 2017/2226²².

17. En l'occurrence, il peut être raisonnablement attendu que l'avant-projet de loi aborde au moins les points suivants :

1° Les autorités nationales compétentes ayant accès aux données de l'EES aux fins d'introduction, de modification, d'effacement et de consultation de données ;

2° La / les finalité(s) pour laquelle / lesquelles chaque autorité compétente a accès aux données de l'EES ;

3° Le responsable central du traitement pour l'EES.

18. Les autorités nationales compétentes aux fins du Règlement EES²³ sont :

- les autorités frontalières entendues comme les garde-frontières chargés, conformément au droit national, d'effectuer des vérifications aux frontières au sens de l'article 2, point 11), du règlement (UE) 2016/399 ;
- les autorités chargées des visas entendues comme les autorités chargées des visas au sens de l'article 4, point 3), du règlement (CE) n° 767/2008, et ;
- les autorités chargées de l'immigration entendues comme les autorités compétentes chargées, conformément au droit national, d'effectuer une ou plusieurs des tâches suivantes:
 - a) vérifier, sur le territoire des États membres, si les conditions d'entrée ou de séjour sur le territoire des États membres sont remplies ;
 - b) examiner les conditions de séjour des ressortissants de pays tiers sur le territoire des États membres et prendre des décisions à ce sujet, dans la mesure où cette autorité n'est pas une «*autorité responsable de la détermination*» au sens de l'article 2, point f), de la directive 2013/32/UE du Parlement européen et du Conseil et, le cas échéant, fournir des conseils conformément au règlement (CE) n° 377/2004 du Conseil ;
 - c) assurer le retour de ressortissants de pays tiers vers un pays tiers d'origine ou de transit.

19. L'article 9 du Règlement EES indique que l'accès à l'EES afin d'introduire, de modifier, d'effacer et de consulter les données visées aux articles 14, 16 à 20 est exclusivement réservé au personnel dûment autorisé des autorités nationales de chaque Etat membre qui sont compétentes pour les finalités définies aux articles 23 à 35 du même règlement.

²¹ Règlement (UE) 2017/2225 du Parlement européen et du Conseil du 30 novembre 2017 modifiant le règlement (UE) 2016/399 en ce qui concerne l'utilisation du système d'entrée/de sortie.

²² Article 2 de l'avant-projet de loi.

²³ Articles 3 et 9 du Règlement EES.

Les Etats membres doivent désigner les autorités nationales compétentes pouvant accéder à l'EES²⁴.

20. L'Organe de contrôle se demande quelles sont ces autorités et ne trouve pas de réponse claire à cette question dans l'avant-projet de loi, ni dans l'Exposé des motifs.

En effet, l'avant-projet de loi fait une fois référence aux services de police²⁵ et une fois référence aux autorités chargées du contrôle aux frontières²⁶, pour le reste, "*d'autres autorités nationales*"²⁷ sont mentionnées.

21. Les autorités nationales compétentes ayant accès aux données de l'EES pour les finalités des articles 23 à 35 du Règlement EES, ou au moins les conditions à remplir pour être considérée comme une telle autorité²⁸, devraient être identifiées dans la loi²⁹.

Considérant que ces autorités peuvent évoluer, celles-ci peuvent être identifiées dans un arrêté royal.

22. Est-ce que par un renvoi général aux "*traitements, en application du Règlement 2017/2226 et de la présente loi, de données stockées dans le EES, effectués par les services de police visés à l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux*"³⁰ dans l'avant-projet de loi, le rédacteur entend que toute entité de police puisse avoir accès aux données de l'EES ? Le rédacteur devrait clarifier ce point.

23. Spécifiquement concernant l'accès aux données de l'EES à des fins répressives, le Règlement EES prévoit la désignation par chaque Etat membre d'autorités compétentes ainsi que d'un point d'accès central³¹ à qui les demandes d'accès à des fins répressives sont adressées³².

Une liste des unités opérationnelles qui, au sein des autorités compétentes désignées, sont autorisées à demander l'accès aux données de l'EES par l'intermédiaire des points d'accès centraux doit également être tenue par chaque Etat membre.

24. En sus des autorités compétentes pour la finalité de l'article 29, le point d'accès central devrait être désigné dans la loi, ou au moins les conditions à remplir pour être considéré comme point d'accès central.

²⁴ Article 9, §2 du Règlement EES.

²⁵ Article 4 de l'avant-projet de loi.

²⁶ Article 5 de l'avant-projet de loi.

²⁷ Article 4 de l'avant-projet de loi.

²⁸ Comme cela est le cas à l'article 44/11/9, §2 LFP par exemple.

²⁹ Voyez paragraphe 14 du présent avis.

³⁰ Article 2/2, §1^{er} inséré par l'article 4 de l'avant-projet de loi.

³¹ A toutes fins utiles, l'article 29 du Règlement EES précise que les Etats membres peuvent désigner plusieurs points d'accès centraux afin de tenir compte de leurs structures organisationnelles et administratives dans l'accomplissement de leurs obligations constitutionnelles ou légales.

³² Articles 31 et 32 du Règlement EES.

25. Prenant en compte le caractère potentiellement technique / sensible de certaines informations³³, l'Organe de contrôle ne voit pas d'inconvénient à ce que les unités opérationnelles, qui au sein des autorités désignées, sont autorisées à demander l'accès aux données de l'EES par l'intermédiaire du point d'accès central, de même que les modalités de communication³⁴ des données de l'EES pour lesquelles l'accès a été demandé soient identifiées dans des directives à diffusion restreinte.

26. Comme indiqué ci-dessus, les Etats membres doivent désigner les autorités nationales compétentes pouvant accéder à l'EES, mais ils sont aussi chargés de préciser à quelle(s) fin(s) chaque autorité a accès aux données de l'EES³⁵.

27. Les finalités d'accès aux données de l'EES pertinentes pour la présente analyse sont les suivantes :

- Utilisation par les autorités frontalières des données à des fins de vérification aux frontières auxquelles l'EES est mis en œuvre³⁶ ;
- Utilisation par les autorités chargées des visas de l'EES aux fins de l'examen des demandes de visa et des décisions y afférentes³⁷ ;
- Utilisation par les autorités compétentes visées à l'article 8 quinquies du Règlement 2016/399 de l'EES aux fins de l'examen des demandes d'accès aux programmes nationaux d'allègement des formalités³⁸ ;
- Accès par les autorités chargées de l'immigration aux données à des fins de vérifications sur le territoire des Etats membres³⁹ ;
- Accès par les autorités frontalières ou les autorités chargées de l'immigration aux données aux fins d'identification⁴⁰ ;
- Consultation des données de l'EES par les autorités désignées par les Etats membres aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière⁴¹.

28. A cet égard, il est clair que la prévention et la détection des infractions terroristes ou d'autres infractions pénales graves ainsi que les enquêtes en la matière (finalités de l'article 29) font partie des missions des services de police tels que visés à l'article 2, 2^o de la loi du 7 décembre 1998⁴² (LPI).

³³ Par exemple les modalités visées à l'article 38 du Règlement EES concernant l'accès aux données de l'EES à des fins répressives.

³⁴ Article 31 du Règlement EES.

³⁵ Article 9, §2 du Règlement EES.

³⁶ Article 23 du Règlement EES.

³⁷ Article 24 du Règlement EES.

³⁸ Article 25 du Règlement EES.

³⁹ Article 26 du Règlement EES.

⁴⁰ Article 27 du Règlement EES.

⁴¹ Article 29 du Règlement EES.

⁴² Loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (LPI).

29. A côté de cela, l'arrêté royal du 14 novembre 2006⁴³ désigne la Direction générale de la police administrative comme autorité compétente en matière de contrôles aux frontières⁴⁴.

30. En outre, l'article 21, alinéa 1^{er} LFP charge les services de police de veiller au respect des dispositions légales relatives à l'accès au territoire, au séjour, à l'établissement et à l'éloignement des étrangers⁴⁵. Le commentaire de l'article 6 de l'avant-projet de loi indique d'ailleurs que, dans le cadre de l'exécution des articles 21 et 34, §3 LFP, les services de police sont considérés comme "*autorité chargée de l'immigration*".

31. Il est compréhensible qu'une autorité compétente désignée ait accès aux données de l'EES pour plusieurs des finalités détaillées ci-dessus. Si le rédacteur souhaite désigner une autorité compétente pour plusieurs finalités, il devrait clarifier ce point.

32. Conformément aux éléments repris dans l'arrêt de la Cour constitutionnelle précité, les finalités d'accès aux données de l'EES pour lesquelles chacune des autorités compétentes est désignée devraient également précisément être identifiées dans la loi.

33. Etant donné que la finalité du traitement a une incidence sur les principes, règles et garanties applicables en matière de protection des données mais aussi sur les modalités de cet accès, le rédacteur de l'avant-projet de loi doit clairement identifier pour quelle(s) finalité(s), les services de police peuvent accéder à l'EES.

En effet, outre le Titre 2 LPD et la LFP, les traitements dans le cadre de l'EES à des fins répressives (article 29) doivent respecter les modalités de procédure, conditions et obligations reprises aux articles 31, 32, 58 et 59 du Règlement EES.

34. Le Règlement EES précise que le RGPD s'applique aux traitements de données effectués par les autorités compétentes au sens de ce règlement, à l'exception des traitements effectués aux fins de l'article 29. Ces derniers tombent sous le champ de la *LED*⁴⁶.

35. L'avant-projet de loi désigne le ministre de l'Intérieur et le ministre de la Justice, chacun dans le cadre de leurs compétences, comme responsables conjoints des traitements, en application du Règlement (EU) 2017/2226 et de la présente loi, de données stockées dans le EES, effectués par les

⁴³ Article 8 de l'Arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale.

⁴⁴ La police fédérale est d'ailleurs reprise sur la liste des services nationaux chargés du contrôle aux frontières au sens de l'article 2, 11) du Règlement 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).

⁴⁵ L'article 21, alinéa 2 LFP prévoit que les services de police se saisissent des étrangers qui ne sont pas porteurs des pièces d'identité ou des documents requis par la réglementation sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, et prennent à leur égard les mesures prescrites par la loi ou par l'autorité compétente.

⁴⁶ Articles 49 et 58 du Règlement EES.

services de police visés à l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux⁴⁷.

36. Il n'est pas clair pour l'Organe de contrôle que le ministre de la Justice soit au courant de sa désignation comme responsable du traitement dans l'avant-projet de loi.

Au vu de son implication évidente pour la question de la responsabilité du traitement et du fait que l'avant-projet de loi touche directement à ses compétences, il y a lieu que le ministre de la Justice signe également l'avant-projet de loi.

37. L'article 39 du Chapitre relatif au développement, au fonctionnement et aux responsabilités du Règlement EES prévoit que chaque état membre désigne une autorité comme responsable central⁴⁸ du traitement au sens de l'article 4, 7) RGPD.

38. Un récent avis du COC relatif à un avant-projet de loi mettant en œuvre le nouveau cadre SIS⁴⁹ a été l'occasion de soulever la question de la désignation au niveau national (central) d'un responsable du traitement pour le N.SIS⁵⁰ considéré comme un système d'information, plutôt que la désignation des ministres respectivement compétents comme responsables du traitement distincts – pas conjoints – selon les autorités nationales qui traitent des données dans le cadre du SIS.

39. Cependant, l'article 4 de l'avant-projet de loi désigne plusieurs responsables du traitement :

"Art. 4. Dans la même loi, il est inséré un article 2/2, rédigé comme suit :

Art. 2/2. §1 Pour les traitements, en application du Règlement (EU) 2017/2226 et de la présente loi, de données stockées dans le EES, effectués par les services de police visés à l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, le ministre de l'Intérieur et le ministre de la Justice sont conjointement responsables du traitement, chacun dans le cadre de leurs compétences.

§ 2. Pour les traitements, en application du Règlement (EU) 201[7] /2226 et de la présente loi, de données stockées dans le EES, effectués par les autres autorités nationales, le responsable du traitement est le ministre sous la compétence duquel l'autorité nationale concernée est placée."

Il s'agit du seul article relatif au responsable du traitement dans l'avant-projet de loi.

⁴⁷ Article 4 de l'avant-projet de loi.

⁴⁸ Soulignement propre.

⁴⁹ Avis de l'Organe de contrôle de l'information policière relatif à un avant-projet de loi relatif au fonctionnement et à l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, dans le domaine des vérifications aux frontières et aux fins du retour des ressortissants de pays tiers en séjour irrégulier, DA220017, 4 juillet 2022.

⁵⁰ Le N.SIS est constitué des systèmes de données nationaux reliés au SIS central, ainsi que d'une infrastructure de communication fournissant un réseau virtuel crypté consacré aux données du SIS et à l'échange de données entre les bureaux SIRENE (voyez les Règlements 2018/1861 et 2018/1862 précités).

40. L'Organe de contrôle se demande si l'article 4 de l'avant-projet de loi constitue la désignation du responsable central du traitement au sens de l'article 39 du Règlement EES ? Le rédacteur de l'avant-projet de loi devrait éclaircir ce point étant donné que le responsable central du traitement doit clairement être désigné dans la loi.

Cette désignation pourrait être l'opportunité d'identifier quelle autorité sera, au niveau national, responsable de certaines obligations telles que celles identifiées aux articles 38, 46 et 50 du Règlement EES en particulier.

41. L'Organe de contrôle souligne que la question du responsable du traitement formulée ci-dessus est liée à celle de la désignation d'un *DPO (Data Protection Officer)*: un DPO sera-t-il désigné pour les accès de la Belgique aux données de l'EES ?

Un DPO *desk ou office*⁵¹ sera-t-il plutôt désigné au niveau national pour les traitements de données effectués dans le cadre de l'EES, disposant de points de contacts au niveau des autorités nationales impliquées ?

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

invite le demandeur à tenir compte des remarques susmentionnées aux paragraphes 8, 9 et 17 ;

invite le demandeur à donner suite aux remarques et questions formulées aux paragraphes 21, 22, 24, 25, 31 à 33, 36, 40 et 41.

Avis approuvé par l'Organe de contrôle de l'information policière le 4 juillet 2022.

Pour l'Organe de contrôle,
Le Président,
(sé.) Philippe ARNOULD

⁵¹ Comme cela est déjà mis en place au sein de certaines entités de police par exemple.