



## ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

| Votre référence | Notre référence | Annexe(s) | Date      |
|-----------------|-----------------|-----------|-----------|
|                 | DA220017        |           | 4.07.2022 |

**Objet : 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**

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<sup>e</sup> 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, reçue par 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 2016/679<sup>1</sup> et de la Directive 2016/680<sup>2</sup>, 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<sup>o</sup>, 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<sup>er</sup>, 2<sup>e</sup> 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<sup>er</sup> (pour les traitements non opérationnels)<sup>3</sup> et du Titre 2 (pour les traitements opérationnels) de la LPD<sup>4</sup>. 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 police<sup>5</sup>.

**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

<sup>1</sup> 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 »).

<sup>2</sup> 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)*).

<sup>3</sup> Article 4 §2, 4<sup>e</sup> alinéa de la LPD.

<sup>4</sup> Article 71 §1<sup>er</sup>, 3<sup>e</sup> alinéa de la LPD.

<sup>5</sup> Articles 59 §1<sup>er</sup>, 2<sup>e</sup> 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 lois<sup>6</sup>.

**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 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 (ci-après 'l'avant-projet de loi').

**6.** Le ministre ayant l'Intérieur dans ses attributions 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.

Le COC a pris connaissance de l'avant-projet de loi et a pris contact avec le demandeur le 21 juin 2022 afin de demander une information complémentaire. Au jour de la remise du présent avis, le demandeur n'avait fourni aucune réponse à l'Organe de contrôle.

**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 policières<sup>7</sup> 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.

---

<sup>6</sup> Article 71, §1<sup>er</sup>, troisième alinéa *juncto* article 236, §3 de la LPD.

<sup>7</sup> Voyez le rapport d'activités 2020 du COC, [https://www.organedecontrole.be/files/Rapport-dactivite\\_COC\\_2020\\_F.pdf](https://www.organedecontrole.be/files/Rapport-dactivite_COC_2020_F.pdf), paragraphes 7 et 8.

### III. Analyse de la demande

**8.** Le Système d'Information Schengen (SIS) a été créé en vertu des dispositions de la Convention d'application de l'accord Schengen (CAAS)<sup>8</sup>.

Un SIS de deuxième génération ('SIS II'), remplaçant le SIS, a été développé sur base de la Décision-cadre 2007/533/JAI<sup>9</sup> et du Règlement 1987/2006<sup>10</sup>.

En 2018, trois règlements (nouveau cadre SIS) qui remplacent progressivement la Décision-cadre 2007/533 et le Règlement 1987/2006 ont été adoptés<sup>11</sup> :

- Le Règlement 2018/1862<sup>12</sup> qui concerne le domaine de la coopération policière et la coopération judiciaire en matière pénale ;
- Le Règlement 2018/1861<sup>13</sup> qui concerne le domaine des contrôles aux frontières ;
- Le Règlement 2018/1860<sup>14</sup> qui concerne le rapatriement de ressortissants de pays tiers séjournant illégalement.

**9.** L'entrée en application de ce nouveau cadre SIS est soumise à plusieurs conditions, en particulier les conditions inscrites aux articles 66 du Règlement 2018/1861 et 79 du Règlement 2018/1862.

En effet, leur entrée en application est conditionnée à la date fixée par la Commission européenne, cette décision étant soumise à la vérification du respect des conditions suivantes :

- 1) Les actes d'exécution nécessaires à l'application des règlements en question ont été adoptés ;
- 2) Les États membres ont informé la Commission qu'ils ont pris les dispositions techniques et juridiques nécessaires pour traiter les données du SIS et échanger des informations supplémentaires en vertu du présent règlement et ;
- 3) L'eu-LISA a informé la Commission de l'achèvement concluant de toutes les activités de test concernant le CS-SIS et l'interaction entre le CS-SIS et les N.SIS.

<sup>8</sup> Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO L 239 du 22 septembre 2000.

<sup>9</sup> Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

<sup>10</sup> Règlement (CE) 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

<sup>11</sup> Système d'information Schengen de deuxième génération (SIS II), <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM:l14544>, consulté le 22 juin 2022.

<sup>12</sup> 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.

<sup>13</sup> 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.

<sup>14</sup> 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.

**10.** L'entrée en application était attendue pour le 28 décembre 2021 au plus tard. Cependant, comme il ressort du dernier rapport<sup>15</sup> sur l'état d'avancement des préparations pour la mise en œuvre complète des nouvelles bases juridiques du système d'information Schengen (SIS)<sup>16</sup>, toutes les conditions pour que la Commission puisse fixer la date de mise en service du SIS ne sont pas encore réunies.

**11.** L'Organe de contrôle comprend que l'avant-projet de loi qui fait l'objet du présent avis fait partie des dispositions juridiques à mettre en œuvre au niveau national pour traiter les données du SIS et échanger des informations supplémentaires en vertu du nouveau cadre SIS.

**12.** Le COC salue l'initiative de l'avant-projet de loi et s'attend à ce que celui-ci réponde aux remarques générales formulées par l'Organe de contrôle et l'Autorité de protection des données dans leur rapport de visite du bureau SIRENE du 12 février 2020<sup>17</sup>.

**13. Cependant, au vu du projet de grande ampleur "smart borders package"<sup>18</sup> en cours, de la prochaine mise en œuvre des règlements relatifs à l'interopérabilité<sup>19</sup>, au système d'entrée et de sortie (EES<sup>20</sup>) et du système ETIAS<sup>21</sup>, ainsi que de leurs conséquences et implications juridiques et techniques au niveau national, et en ayant égard à différentes demandes d'avis qu'il a reçues ces derniers mois<sup>22</sup>, l'Organe de contrôle rejoint l'avis de l'Inspection des finances sur l'avant-projet de loi et se demande même, de manière plus**

<sup>15</sup> Rapport de la Commission au Parlement européen et au Conseil du 29 juin 2021 sur l'état d'avancement des préparations pour la mise en œuvre complète des nouvelles bases juridiques du système d'information Schengen (SIS) conformément à l'article 66, paragraphe 4, du règlement (UE) 2018/1861 et à l'article 79, paragraphe 4, du règlement (UE) 2018/1862, COM(2021) 336 final, consultable sur <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021DC0336>.

<sup>16</sup> Conformément à l'article 66, paragraphe 4, du Règlement 2018/1861 et à l'article 79, paragraphe 4, du Règlement 2018/1862.

<sup>17</sup> Voyez le Rapport sur le contrôle et la visite de la Direction de la Coopération Internationale Policière de la police fédérale par l'Organe de contrôle de l'information policière dans le cadre de ses compétences de contrôle et de suivi, 12 février 2020, la version publique du rapport est consultable sur [https://www.organedecontrôle.be/files/DIO190001\\_Visite\\_PF\\_CGI\\_Publique\\_F.PDF](https://www.organedecontrôle.be/files/DIO190001_Visite_PF_CGI_Publique_F.PDF).

<sup>18</sup> 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](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).

<sup>19</sup> 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.

<sup>20</sup> Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) no 767/2008 et (UE) no 1077/2011.

<sup>21</sup> 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.

<sup>22</sup> Outre la présente demande d'avis, notamment: une demande d'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 (référence COC, DA220016) ; 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).

**générale, si un travail de révision et de mise en conformité davantage intégré au niveau national n'aurait pas été plus opportun.**

**14.** Pour le présent avis, l'Organe de contrôle comprend tant le traitement de données relatives au signalement SIS que l'échange d'informations supplémentaires sous les termes "traitements (de données et d'informations) dans le cadre du SIS".

**15.** Les traitements de données à caractère personnel exécutés dans le cadre du SIS doivent être conformes aux dispositions du RGPD et/ou de la Directive police-justice<sup>23</sup>, *in concreto* au Titre 2 LPD et à la LFP en particulier pour ce qui concerne les services de police.

**16.** 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 2022<sup>24</sup> 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 (considérant B.13.2).

<sup>23</sup> Article 51 du Règlement 2018/1861 et article 66 du Règlement 2018/1862.

<sup>24</sup> Cour constitutionnelle, arrêt n° 33/2022 du 10 mars 2022, [www.courconstitutionnelle.be](http://www.courconstitutionnelle.be).

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) (considérant B.13.2).

**17.** Une fois entré en application, le nouveau cadre SIS sera d'application directe en droit belge. Dans les cas où ce nouveau cadre SIS 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 dans la loi belge en des termes clairs et suffisamment précis, tenant évidemment compte de la sensibilité et de la spécificité de la matière concernée.

L'avant-projet de loi faisant l'objet du présent avis a pour ambition de mettre en œuvre les Règlements SIS et de définir les modalités relatives au fonctionnement et à l'utilisation du SIS par les services publics belges<sup>25</sup>.

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

- 1° La désignation de l'Office N.SIS pour la Belgique ;**
- 2° La désignation du bureau SIRENE pour la Belgique ;**
- 3° Les autorités nationales compétentes ayant accès aux données du SIS ;**
- 4° Le responsable du traitement ;**
- 5° Les délais de conservation.**

**19.** L'article 2 de l'avant-projet de loi fournit la définition de certains termes qui sont pourtant déjà définis dans les Règlements SIS comme le "CS-SIS", le "N.SIS", "le bureau SIRENE" et "l'Office N. SIS". Ces définitions qui sont plutôt des paraphrases n'apportent aucune plus-value à l'avant-projet. Vu l'effet direct d'un règlement européen, il est même en principe interdit de répéter comme telles des règles de droit européen dans la législation belge<sup>26</sup>.

Cependant, certains termes utilisés ne font l'objet d'aucune définition comme par exemple "autorités nationales<sup>27</sup>" ou encore "autorités signalantes<sup>28</sup>".

---

<sup>25</sup> Article 3 de l'avant-projet de loi.

<sup>26</sup> Voir Avis d'initiative du 21/2017 du 3 mai 2017 de l'Autorité de protection des données (anciennement la Commission de la protection de la vie privée) relatif au projet de loi réformant la Commission de la protection de la vie privée, Chambre, DOC 54, 2016-2017, n° 2648/001, point 29.

<sup>27</sup> Chapitre 2 de l'avant-projet de loi.

<sup>28</sup> Chapitre 2 de l'avant-projet de loi.

**Il est préférable de ne définir dans l'avant-projet que les termes qui ne sont pas définis dans le nouveau cadre SIS et qui sont pertinents au regard de l'avant-projet de loi.**

**20.** Le Titre 2 de l'avant-projet de loi contient deux chapitres, le premier relatif aux Offices SIS et le second relatif aux autorités nationales.

En application des articles 7 des Règlements 2018/1861 et 2018/1862, les articles 4 et 5 du Chapitre 1<sup>er</sup> de l'avant-projet de loi désignent l'Office N.SIS et le bureau SIRENE pour la Belgique.

L'Organe de contrôle salue cette désignation qui constitue "*une confirmation légale de la répartition initiale des tâches telle que définie au niveau national lors de l'établissement du SIS, bien que celle-ci n'ait jamais été ancrée dans la législation nationale*"<sup>29</sup>, et qui met un terme au silence du droit belge identifié dans le rapport de visite de l'Organe de contrôle et l'Autorité de protection des données du bureau SIRENE du 12 février 2020<sup>30</sup>.

**21.** Le Chapitre 2 (articles 6 à 10) de l'avant-projet de loi concerne les autorités nationales.

Cet article prévoit des obligations en matière de confidentialité, de tenue de registres de journalisation, d'établissement de statistiques, de responsabilités en matière d'exactitude et d'actualisation de données, de licéité et de formation du personnel.

**22.** En sus de sa remarque relative aux définitions pertinentes pour l'avant-projet de loi<sup>31</sup>, l'Organe de contrôle se demande qui sont les "*autorités nationales*" et les "*autorités signalantes*" visées par ce Chapitre 2 et pour quelles finalités (Titre 2 LPD ? RGPD ? Titre 3 LPD ?) ces autorités traitent-elles des données dans le cadre du SIS ?

S'agit-il des services de police au sens de l'article 2, 2<sup>o</sup> de la loi du 7 décembre 1998<sup>32</sup> (LPI), des autorités compétentes visées à l'article 26, 7<sup>o</sup> de la LPD et/ou d'autres autorités ?

**23.** Le commentaire des articles fait tantôt référence à des articles du Titre 2 LPD<sup>33</sup> qui ne s'appliquent qu'à l'égard de certaines "*autorités compétentes*" au sens de l'article 26, 7<sup>o</sup> LPD, tantôt uniquement référence au RGPD<sup>34</sup>.

La lecture des articles 34 du Règlement 2018/1861 et 44 du Règlement 2018/1862 révèle pourtant que les autorités nationales comprennent *a minima* des autorités compétentes au sens du Titre 2 LPD (les services de la police intégrée, structurée à deux niveaux) et des autorités tombant sous le champ du

<sup>29</sup> Exposé des motifs de l'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.

<sup>30</sup> Rapport DIO19001, *op. cit.*

<sup>31</sup> Voir paragraphe 19 du présent avis.

<sup>32</sup> Loi du 7 décembre 1998 organisant un service de police intégré, structurée à deux niveaux.

<sup>33</sup> A titre d'exemple : commentaires des articles 7 (registre de journalisation) et 9 (qualité et exactitude des données) de l'avant-projet de loi.

<sup>34</sup> A titre d'exemple : commentaire de l'article 11 de l'avant-projet de loi relatif au responsable du traitement.



RGPD (p. ex. l'Office des étrangers). L'avant-projet de loi cite d'ailleurs les services de police au sens de l'article 2, 2° LPI et l'Office des étrangers.

L'Organe de contrôle déduit que ces autorités font partie des autorités nationales visées dans le Chapitre 2 de l'avant-projet de loi.

**24. Les autorités nationales compétentes traitant des données dans le cadre du SIS, ou au moins les conditions à remplir pour être considéré comme une autorité nationale compétente au sens du nouveau cadre SIS<sup>35</sup>, devraient être identifiées dans la loi<sup>36</sup>. Vu *«le nombre d'autorités nationales (et donc de personnes) ayant accès à des données du SIS ou à des informations supplémentaires ne cessant de croître»<sup>37</sup>, ces autorités peuvent être identifiées dans un arrêté royal.***

**25.** L'article 7 de l'avant-projet de loi impose la tenue d'un fichier de journalisation à chaque autorité nationale.

Le commentaire des articles insiste sur l'importance de la répartition de la responsabilité nationale entre les différentes autorités nationales directement connectées au SIS, précisant que chaque autorité nationale disposant de sa (propre) connexion directe au SIS se porte en principe garante de l'enregistrement et de la conservation des données de journalisation.

L'Organe de contrôle remarque que le commentaire de l'article 7 de l'avant-projet de loi renvoie exclusivement à l'article 56 de la LPD relatif à l'obligation de tenue d'un fichier de journalisation et attire l'attention sur le fait que cet article s'applique exclusivement aux autorités compétentes visées à l'article 26, 7° de la LPD alors que l'article 7 lui-même renvoie aux articles 12 des Règlements 2018/1861 et 2018/1862 qui prévoient tous les deux une obligation (générale) de tenue de registre des journalisation envers les Etats membres.

**26.** Considérant que l'objectif de l'article 7 quant à la répartition des responsabilités en matière de tenue des registres n'est pas atteint étant donné que les autorités nationales ne sont pas définies ni identifiées, le rédacteur de l'avant-projet de loi devrait apporter davantage de clarté, aussi en ayant égard à la remarque formulée au paragraphe 24.

**27. Le commentaire de cet article indique que ces registres doivent être mis à la disposition de l'instance disciplinaire de chaque autorité nationale. Il doit être clair que les fichiers de journalisation doivent pouvoir être mis à disposition des autorités de contrôle et de protection des données compétentes dans le cadre et pour l'exercice de leurs missions<sup>38</sup>.**

<sup>35</sup> Comme cela est le cas à l'article 44/11/9, §2 LFP par exemple.

<sup>36</sup> Voyez paragraphe 16 du présent avis.

<sup>37</sup> Commentaire de l'article 6 de l'avant-projet de loi.

<sup>38</sup> Articles 66 LCA, 244 LPD, 55 du Règlement 2018/1861 et 13 Règlement 2018/1862.

**28.** L'article 8 de l'avant-projet de loi porte sur la production de statistiques qui est confiée aux "*autorités signalantes*", respectivement pour leurs propres signalements.

Cet article fait références aux obligations inscrites aux articles 39, §6 du Règlement 2018/1861 et 53, §8 et 54, §6 du Règlement 2018/1862 mais le commentaire de cet article élargit cette obligation (contenu et destinataires), en référence aux articles 60 du Règlement 2018/1861 et 74 du Règlement 2018/1862.

Le commentaire insiste à nouveau sur l'importance de la répartition de la responsabilité nationale entre les différentes autorités nationales, chacune pour ses propres statistiques.

**29. En sus de la remarque déjà formulée aux paragraphes 24 et 26, le rédacteur de l'avant-projet de loi devrait apporter davantage de clarté quant à ses attentes relatives à la production de statistiques par les différents acteurs impliqués dans les traitements de données du SIS : qui doit produire quelles statistiques et les mettre à disposition de qui, pour quelles finalités ?**

**30. Il y a également lieu de clairement identifier qui, pour la Belgique, est chargé de rassembler les statistiques visées aux articles 31 et 39, §6 du Règlement 2018/1861 et aux articles 26, §4, 53, §8 et 54, §6 du Règlement 2018/1862, et qui est chargé, pour la Belgique, de recueillir les informations nécessaires pour l'établissement par eu-LISA des rapports visés à l'article 60 du Règlement 2018/1861 et à l'article 74 du Règlement 2018/1862.**

**31. Eu égard au fait que le développement et l'élaboration d'un programme de formation national ne soit pas encore mis en place<sup>39</sup>, l'Organe de contrôle ne perçoit pas la plus-value de l'article 10 de l'avant-projet de loi qui semble plutôt être une paraphrase de l'article 14 des Règlements 2018/1861 et 2018/1862 (voir aussi n° 19 du présent avis).**

**32.** Le Titre 3 de l'avant-projet de loi concerne les aspects de protection des données à caractère personnel, le premier chapitre portant sur le responsable du traitement et le second se rapportant aux durées de conservation.

**33.** L'article 4 des Règlements 2018/1861 et 2018/1862 indique que le SIS se compose d'un système central (SIS central) et de systèmes nationaux (N.SIS).

---

<sup>39</sup> Commentaire de l'article 10 de l'avant-projet de loi.

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.

Les autorités compétentes introduisent, mettent à jour, suppriment et effectuent des recherches dans les données du SIS par l'intermédiaire de leur propre N.SIS, auquel s'applique le droit national<sup>40</sup>.

**34. Le nouveau cadre SIS<sup>41</sup> charge l'Office N.SIS et le bureau SIRENE de tâches en termes de qualité des données (coordination de la vérification de la qualité des données pour le bureau SIRENE<sup>42</sup>), de responsabilité du bon fonctionnement, de sécurité et de disponibilité pour le N.SIS.**

**A cet égard, considérant le N.SIS comme un système d'information, et au même titre que l'Office N.SIS et le bureau SIRENE assument au niveau national pour tout le système d'information N.SIS les tâches qui leurs incombent, la question de la désignation au niveau national d'un responsable du traitement pour le N.SIS, plutôt que la désignation dans l'avant-projet de loi<sup>43</sup> des ministres respectivement compétents comme responsables du traitement distincts – pas conjoints – selon les autorités nationales – non définies et non identifiées – qui traitent des données dans le cadre du SIS mérite d'être posée.**

**Les avantages que cela pourrait représenter en termes de sécurité juridique<sup>44</sup> et de prévisibilité devraient être évalués.**

**Cela n'empêcherait pas que les autorités nationales compétentes soient naturellement chacune responsables de la qualité, de l'exactitude et de l'actualisation des données qu'elles traitent dans le cadre du SIS<sup>45</sup>.**

**35.** Dans son rapport de visite du bureau SIRENE du 12 février 2020<sup>46</sup>, l'Organe de contrôle avait mis en évidence l'importance du rôle du Délégué à la protection des données (DPO<sup>47</sup>).

L'Organe de contrôle souligne que la question du responsable du traitement formulée ci-dessus est liée à celle de la désignation d'un Délégué à la protection des données (DPO) : un DPO sera-t-il désigné pour le bureau SIRENE et pour l'Office N.SIS ainsi que pour chaque autorité nationale ?

<sup>40</sup> Article 41, §9 du Règlement 2018/1861 et article 56, §8 du Règlement 2018/1862.

<sup>41</sup> Cela était déjà le cas avec la Décision-cadre 2007/533/JAI et le Règlement 1987/2006.

<sup>42</sup> Article 7, §2, alinéa 3 des Règlements 2018/1861 et 2018/1862.

<sup>43</sup> Article 11 de l'avant-projet de loi.

<sup>44</sup> A titre d'exemple : les procédures en cas de fuite de données, l'établissement et/ou la correspondance des plans de sécurité,

...

<sup>45</sup> Titre 2, Chapitre 2 "Autorités nationales" de l'avant-projet de loi.

<sup>46</sup> Rapport DIO19001, *op. cit.*

<sup>47</sup> *Data Protection Officer.*

Un DPO « *desk* » ou « *office* »<sup>48</sup> sera-t-il plutôt désigné au niveau national pour les traitements de données effectués dans le cadre du SIS, disposant de points de contacts au niveau du bureau SIRENE, de l'Office N.SIS et des autorités nationales impliquées ?

**36.** En matière de conservation des données dans le cadre du SIS, il y a lieu de faire une double distinction: d'une part, entre les données liées aux signalements en tant que tels et les informations supplémentaires rattachées aux signalements, et d'autre part, il faut faire la différence entre les données relatives à un signalement national, les données relatives à un signalement étranger et celles relatives à un signalement étranger pour lequel une mesure a été prise sur le territoire belge.

De manière générale, les signalements SIS obéissent à un **principe de proportionnalité**<sup>49</sup> et un **principe de nécessité**<sup>50</sup> qui veulent que le signalement ne soit conservé que pendant le temps nécessaire à la réalisation des finalités pour lesquelles il a été introduit.

**37.** Un signalement a une durée de conservation limitée déterminée dans les Règlements 2018/1861 et 2018/1862. Ces délais sont maximums et de stricte application de sorte qu'à leur échéance et sans décision expresse de prolongation de la part de l'autorité compétente, le signalement est automatiquement effacé.

Les Règlements 2018/1861 et 2018/1862 fixent respectivement le délai endéans lequel un réexamen de la nécessité de conserver le signalement doit être effectué. Au terme de cet examen, une décision de prolongation peut être communiquée.

**38.** Les Règlements 2018/1861 et 2018/1862 prévoient la possibilité de conserver dans des fichiers nationaux des données du SIS sur la base desquelles la conduite a été exécutée sur le territoire national, pour **une durée maximale de trois ans, sauf si le droit national détermine des délais plus courts**. Cette possibilité de conservation est également ouverte pour les données concernant les signalements nationaux, sans que les Règlements précités ne fixent de délai de conservation.

**39.** En outre, les Règlements 2018/1861 et 2018/1862<sup>51</sup> prévoient que "*les Etats membres veillent à ce que tous les accès à des données à caractère personnel et tous les échanges de données à caractère personnel au sein du CS-SIS soient enregistrés dans leur N.SIS afin de pouvoir contrôler la licéité de la recherche et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS et de garantir l'intégrité et la sécurité des données.*"

Ces registres doivent en particulier indiquer l'historique du signalement, la date et l'heure de l'opération de traitement des données, les données utilisées pour effectuer une recherche, la référence aux données traitées et les identifiants d'utilisateur individuels et uniques de l'autorité compétente et de la personne

<sup>48</sup> Comme cela est déjà mis en place au sein de certaines entités de police par exemple.

<sup>49</sup> Articles 21 des Règlements 2018/1861 et 2018/1862.

<sup>50</sup> Articles 39, §1<sup>er</sup> et 40 du Règlement 2018/1861 et articles 53, §1<sup>er</sup> et 55 du Règlement 2018/1862.

<sup>51</sup> Articles 12, §1<sup>er</sup>.

traitant les données. Il est prévu que ces registres soient supprimés **trois ans après leur création** et que les registres contenant l'historique des signalements soient supprimés **trois ans après la suppression des signalements**.

**40.** En ce qui concerne la conservation des informations supplémentaires, les Règlements 2018/1861 et 2018/1862 prévoient que le bureau SIRENE conserve une trace des décisions ayant donné lieu à un signalement, afin de faciliter l'échange d'informations supplémentaires.

Les données à caractère personnel conservées au sein du bureau SIRENE à la suite d'un échange d'informations ne sont conservées que pendant le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été fournies. Elles sont, en tout état de cause, supprimées **au plus tard un an après que le signalement correspondant a été supprimé du SIS**.

En outre, il est possible de conserver, dans des fichiers nationaux, des données relatives à un signalement particulier que l'État membre a introduit ou à un signalement sur la base duquel une conduite a été exécutée sur son territoire. **Le délai pendant lequel les données peuvent être conservées dans ces fichiers est régi par le droit national**.

**41.** La Décision-cadre 2007/533/JAI et le Règlement 1987/2006 prévoyaient des règles similaires. L'absence de dispositions nationales complétant ces dispositions avait fait l'objet d'observations et de remarques dans le rapport de visite de l'Organe de contrôle et de l'APD du 12 février 2020<sup>52</sup>.

**42.** L'article 12 de l'avant-projet de loi concerne les délais de conservation applicables aux données du SIS, c'est-à-dire les données qui constituent un signalement<sup>53</sup> ainsi que ceux applicables aux informations supplémentaires. Ces informations ne font pas partie des données qui constituent un signalement stockées dans le SIS mais sont en rapport avec ces signalements et doivent être échangées par l'intermédiaire des bureaux SIRENE<sup>54</sup>.

**43.** Le libellé de l'article 12 de l'avant-projet de loi induit une confusion importante quant aux banques de données nationales concernées et aux délais de conservation qui leurs sont applicables, sans oublier l'absence perpétuelle déjà mise en évidence de définition / d'identification des autorités nationales concernées qui sont visées dans cet article<sup>55</sup>.

Pour l'analyse de cet article, l'Organe de contrôle se concentre sur les règles applicables aux services de police, laissant le soin à l'Autorité de protection des données de se prononcer sur d'autres aspects (notamment par rapport aux autres autorités nationales) au besoin.

---

<sup>52</sup> Rapport DIO19001, *op. cit.*

<sup>53</sup> Telles que visées aux articles 20 et suivants des Règlements 2018/1861 et 2018/1862.

<sup>54</sup> Articles 3 des Règlements 2018/1861 et 2018/1862.

<sup>55</sup> Voir d'ailleurs remarque au paragraphe 24 du présent avis.

**44. L'Organe de contrôle demande avant toute chose que les traitements effectués dans le cadre du SIS par les services de police au sens de l'article 2, 2° LPI soient clairement différenciés des traitements effectués par le bureau SIRENE et l'Office N.SIS dans le cadre des missions qui leurs sont confiées par le nouveau cadre SIS.**

**En effet, les traitements de ces services de police dans le cadre du SIS ne sont pas les mêmes (finalités), de même que leurs droits d'accès dans le cadre du N.SIS.**

**45.** A la lecture de l'article 12 de l'avant-projet de loi, il apparaît clairement qu'il n'a pas été tenu compte des spécificités détaillées aux paragraphes précédents.

Bien qu'une distinction théorique entre les traitements de données relatives aux signalements et les informations supplémentaires soit établie, les deux premiers paragraphes de l'article 12 prévoient, tant pour les données relatives aux signalements que pour les informations supplémentaires, que le traitement par les services de police ait lieu dans une banque de données policière opérationnelle de type banque de données particulière, tant que celui-ci est nécessaire et pour une durée de conservation de 10 ans maximum.

Rien ne permet au COC d'établir d'où provient ce délai de 10 ans maximum : Ce délai trouve-t-il sa source dans une pratique déjà établie ? Fait-il suite à un avis d'un ou plusieurs délégués à la protection des données compétents ?

*A contrario*, le paragraphe 3 prévoit que les services de police ainsi que toutes les autres autorités nationales puissent traiter les données relatives aux signalements et les informations supplémentaires dans les banques de données nationales qu'ils gèrent, conformément aux règles qui s'appliquent aux banques de données concernées, notamment dans le respect des durées de conservation d'application pour ces banques de données.

**46.** Le commentaire des articles précise concernant les paragraphes 1 et 2 qu'il s'agit bien de banques de données particulières et donc pas de la Banque de données Nationale Générale (BNG) mais indique qu'il peut s'agir de banques de données nationales (particulières) qui auraient été développées spécialement en vue du traitement (opérationnel) de ces données.

**47.** L'Organe de contrôle rappelle que les banques de données particulières telles que visées à l'article 44/2, §1<sup>er</sup>, alinéa 1<sup>er</sup>, 3° LFP sont des banques de données policières opérationnelles. Celles-ci peuvent être créées, dans **des circonstances spécifiques**, dans le but de traiter les données qu'elles contiennent dans le cadre de l'exercice de leurs missions et finalités de police administrative et judiciaire, et que ces données sont supprimées dès que ces besoins particuliers disparaissent.

L'article 44/11/3 LFP précise que la création d'une banque de données particulière est **motivée** par au moins un des besoins particuliers suivants :

- a) La nécessité de classifier des données à caractère personnel ou informations au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité ;
- b) L'impossibilité technique ou fonctionnelle d'alimenter la B.N.G. de tout ou partie des données à caractère personnel et informations traitées dans ces banques de données ;
- c) Le caractère non pertinent ou excessif de la centralisation dans la B.N.G. de tout ou partie des données à caractère personnel ou des informations, dans le cadre de l'exercice des missions de police administrative et de police judiciaire.

**48.** La création d'une banque de données particulière au sens de la LFP requiert la démonstration préalable du respect des conditions de l'article 44/11/3 LFP, ce que ni l'avant-projet de loi ni le commentaire des articles ne fournissent. Il en va de même pour le délai de conservation de 10 ans maximum fixé pour toute catégorie de données confondues, sans justification quant à son caractère nécessaire et proportionné.

**49.** En outre, les paragraphes 4 et 5 de l'article 12 de l'avant-projet de loi prévoient que les durées de conservation applicables commencent à courir à partir du moment où le signalement est supprimé ou arrive à échéance et, qu'au terme des délais de conservation, les données seront détruites sans préjudice des règles d'application en matière d'archivage des données.

Toujours se concentrant sur les implications de ces paragraphes pour les services de police, l'Organe de contrôle souligne que ces paragraphes **ne respectent manifestement pas** les dispositions des Règlements SIS précitées.

L'Organe de contrôle se demande si le renvoi aux règles en matière d'archivage concerne les règles d'archivage établies par la LFP, qui sont en tous les cas applicables uniquement à la BNG et non aux banques de données particulières. Autrement, le rédacteur de l'avant-projet de loi doit préciser à quelles règles d'archivage l'article 12 de l'avant-projet de loi fait référence.

**50. Des éléments exposés ci-dessus, l'Organe de contrôle considère qu'il n'a certainement pas été tenu compte des dispositions du nouveau cadre SIS et du N.SIS en tant que système d'information constitué des systèmes de données nationaux reliés au SIS central, ainsi que d'une infrastructure de communication<sup>56</sup>, qu'il n'a assurément pas été tenu compte du projet en cours au niveau de la GPI<sup>57</sup> relatif à i-Police mettant prochainement à la disposition du bureau SIRENE un *case management system* dont les modalités sont encore floues pour le COC, et que, sans disposer de davantage d'information et de**

<sup>56</sup> Articles 4 des Règlements 2018/1861 et 2018/1862.

<sup>57</sup> Entendre les services de police intégrée, structurée à deux niveaux tels que visés à l'article 2, 2° LPI (Geïntegreerde politie – Police Intégrée).

**justification, les délais de conservation fixés dans l'avant-projet de loi sont manifestement disproportionnés et contraires aux dispositions du nouveau cadre SIS.**

**51. L'Organe de contrôle demande que l'article 12 de l'avant-projet de loi soit revu en ayant égard au nouveau cadre SIS ainsi qu'aux dispositions de la LPD et de la LFP, et demande d'être activement tenu au courant du résultat de cette révision.**

**52.** Le Titre 4 de l'avant-projet de loi concerne les mesures à prendre. Il est constitué d'un chapitre unique "*rapport*" et d'un seul article (article 13).

**53.** Le nouveau cadre SIS prévoit que les signalements sont introduits dans le SIS par les Etats membres, à la demande de l'autorité compétente<sup>58</sup>.

Il est prévu que la Commission européenne adopte des actes d'exécution pour établir et préciser les règles nécessaires à l'introduction, la mise à jour et la suppression des données<sup>59</sup>.

En outre, concernant l'échange d'informations supplémentaires, il y a lieu de se référer au Manuel SIRENE<sup>60</sup> qui est un ensemble d'instructions décrivant en détail les règles et les procédures régissant l'échange bilatéral ou multilatéral des informations supplémentaires<sup>61</sup>.

**54.** Le nouveau cadre SIS n'établit pas de règles précises concernant les modalités pratiques de l'introduction des signalements dans le SIS.

Cependant, l'article 36 du Règlement 2018/1862 indique spécifiquement que les signalements aux fins de contrôle discret, de contrôle d'investigation ou de contrôles spécifiques sont introduits conformément au droit national de l'Etat membre signalant<sup>62</sup>.

Dans le même sens, le rôle du bureau SIRENE dans le réexamen des signalements (procédure de prolongation) peut être déterminé dans le droit national<sup>63</sup>.

**55.** L'article 13 de l'avant-projet de loi – qui est donc de portée générale – se limite à prévoir qu'en cas de *hit*, c'est-à-dire en cas de réponse positive à la suite d'une recherche dans le SIS, le fonctionnaire ou l'autorité publique doit en informer le bureau SIRENE et l'informer également de l'exécution ou non de la conduite à tenir.

<sup>58</sup> Article 24 du Règlement 2018/1861 et articles 26, §1<sup>er</sup>, 32, §1<sup>er</sup>, 34, §1<sup>er</sup>, 36, §§ 1<sup>er</sup> et 4, 38, §1<sup>er</sup> et 40 du Règlement 2018/1862.

<sup>59</sup> Les signalements des articles 26, 32, 34 et 38 du Règlement 2018/1862 sont concernés.

<sup>60</sup> Décision d'exécution (UE) 2017/1528 de la Commission du 31 août 2017 remplaçant l'annexe de la décision d'exécution 2013/115/UE relative au manuel SIRENE et à d'autres mesures d'application pour le système d'information Schengen de deuxième génération (SIS II).

<sup>61</sup> Articles 8 des Règlement 2018/1861 et 2018/1862.

<sup>62</sup> Soulignement propre.

<sup>63</sup> Article 39, §7 du Règlement 2018/1861 et article 59, §9 Règlement 2018/1862.



**56. L'Organe de contrôle remarque cependant que l'article 22 de l'avant-projet de loi prévoit que les modalités des signalements dans le SIS qui devraient à l'avenir directement pouvoir être effectués par l'Office des étrangers peuvent être fixées par Arrêté royal.**

**L'Organe de contrôle considère que cette initiative devrait, dans l'intérêt de la sécurité juridique et de la prévisibilité, être élargie à tous les types de signalements dans le cadre du SIS. Dans l'intérêt de l'exercice des missions de police, l'Organe de contrôle ne voit pas d'inconvénient à ce que les aspects plus techniques / sensibles soient réglés dans des directives à diffusion restreinte.**

**57.** Le nouveau cadre SIS prévoit la possibilité d'introduire un nouveau type de signalement dans le SIS, relatif aux personnes recherchées inconnues à des fins d'identification conformément au droit national<sup>64</sup>.

Le Règlement 2018/1862 prévoit qu'en cas de réponse positive (*Hit*), l'identité de la personne soit établie conformément au droit national, avec vérification par un expert que les données dactyloscopiques dans le SIS appartiennent à la personne.

**58. L'Organe de contrôle se demande si une autorité sera responsable au niveau national de ces vérifications ? Dans l'affirmative, les conditions à remplir par cette autorité devraient au moins être identifiées dans la loi<sup>65</sup> et les modalités pratiques applicables à la procédure de vérification visée à l'article 41 du Règlement 2018/1862 pourraient être reprises dans un arrêté royal, sans préjudice des aspects plus techniques / sensibles qui peuvent être réglés dans des directives à diffusion restreinte.**

**59.** L'article 43 du Règlement 2018/1862 prévoit le traitement de photographies et d'images faciales aux fins d'identification d'une personne dans le contexte des points de passage frontaliers habituels.

**L'Organe de contrôle rappelle que, le fait que le Règlement 2018/1862 prévoit ce type de traitement pour des finalités spécifiques n'empêche pas que la LFP doive être modifiée afin de permettre l'utilisation de la reconnaissance faciale pour les finalités générales de l'exécution de missions de police administrative et de police judiciaire<sup>66</sup>.**

---

<sup>64</sup> Article 40 du Règlement 2018/1862.

<sup>65</sup> Voyez paragraphe 16 du présent avis.

<sup>66</sup> A toutes fins utiles : Avis relatif à une proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés (DOC 55 1349/001 du 16 juin 2020), 24 janvier 2022, DA210029, consultable sur [https://www.organedecontrôle.be/files/DA210029\\_Avis\\_F.pdf](https://www.organedecontrôle.be/files/DA210029_Avis_F.pdf) ; le rapport intermédiaire de l'Organe de contrôle de l'information policière avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'Organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale à l'aéroport national de Zaventem, 16 septembre 2019, DIO19005, version publique disponible sur [https://www.organedecontrôle.be/files/DIO19005\\_Contr%C3%B4le\\_LPABRUNAT\\_Reconnaissance\\_Faciale\\_Publique\\_F.PDF](https://www.organedecontrôle.be/files/DIO19005_Contr%C3%B4le_LPABRUNAT_Reconnaissance_Faciale_Publique_F.PDF).

**PAR CES MOTIFS,**

**l'Organe de contrôle de l'information policière**

**invite le demandeur à tenir compte des remarques susmentionnées aux paragraphes 13, 18, 29, 31 et 43 ;**

**invite le demandeur à donner suite aux remarques et questions formulées aux paragraphes 22, 24, 26, 27, 30, 34, 35, 45, 49, 56 et 58.**

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