COMMISSION
EUROPÉENNE

Bruxelles, le 21.12.2016
COM(2016) 882 final

2016/0408 (COD)

Proposition de

# RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

## sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant le règlement (UE) n° 515/2014 et abrogeant le règlement (CE) n° 1987/2006

# EXPOSÉ DES MOTIFS

## 1. CONTEXTE DE LA PROPOSITION

### • Justification et objectifs de la proposition

Ces deux dernières années, l'Union européenne a travaillé à relever simultanément ces défis en soi que sont la gestion des flux migratoires, une gestion intégrée de ses frontières extérieures et la lutte contre le terrorisme et la criminalité transfrontière. Pour apporter une solution solide à ces défis, il est essentiel que l'échange d'informations entre les États membres, et entre ceux-ci et les agences compétentes de l'Union européenne, soit efficace.

Le système d'information Schengen (SIS) est l'instrument le plus à même de garantir une coopération efficace entre les services de l'immigration, de la police, des douanes et de la justice de l'Union européenne et des pays associés à l'espace Schengen. Les autorités compétentes des États membres, telles que la police, les garde-frontières et les douanes, doivent, en effet, avoir accès à des informations de qualité sur les personnes et les objets qu'elles contrôlent, assorties d'instructions claires sur ce qu'il convient de faire dans chaque cas. Ce système d'information à grande échelle est au cœur même de la coopération Schengen et joue un rôle crucial, en facilitant la libre circulation des personnes dans l'espace Schengen. Il permet aux autorités compétentes de saisir et de consulter des données sur des personnes recherchées, des personnes qui pourraient ne pas avoir le droit de pénétrer ou de séjourner dans l'Union européenne ou des personnes disparues (en particulier des enfants), ainsi que sur des objets qui ont peut-être été volés, détournés ou égarés. Le SIS contient non seulement des informations sur des personnes ou des objets particuliers, mais aussi des instructions claires sur ce que les autorités compétentes sont censées faire une fois une personne ou un objet retrouvé(e).

En 2016, trois ans après la mise en service du SIS de deuxième génération, la Commission a procédé à une évaluation complète du système[1]. Cette évaluation a montré que le SIS était un réel succès opérationnel. En 2015, les autorités nationales compétentes ont réalisé près de 2,9 milliards de vérifications portant sur des personnes et des objets à partir de données figurant dans le SIS et ont échangé plus de 1,8 million d'informations supplémentaires. Néanmoins, ainsi que la Commission l'annonce dans son programme de travail pour 2017, il convient de renforcer encore l'efficacité et l'efficience du système sur la base cette expérience positive. Aussi la Commission présente-t-elle un premier ensemble de trois propositions qui, tirant les leçons de l'évaluation, visent à améliorer le SIS et à en étendre l'utilisation, tout en poursuivant les efforts qu'elle a engagés pour accroître l'interopérabilité des systèmes répressifs et des systèmes de gestion des frontières, dans le droit fil des travaux actuellement menés par le groupe d'experts à haut niveau sur les systèmes d'information et l'interopérabilité.

Ces propositions prévoient l'utilisation du système pour a) la gestion des frontières, b) la coopération policière et la coopération judiciaire en matière pénale et c) le retour des ressortissants de pays tiers en séjour irrégulier. Les deux premières propositions forment ensemble la base juridique de l'établissement, du fonctionnement et de l'utilisation du SIS. La proposition relative à l'utilisation du SIS pour le retour des ressortissants de pays tiers en

---

[1] Rapport d'évaluation du système d'information Schengen de deuxième génération (SIS II) présenté au Parlement européen et au Conseil conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi qu'à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI, et document de travail des services de la Commission l'accompagnant (JO...).

séjour irrégulier complète les dispositions contenues dans la proposition relative à la gestion des frontières. Elle prévoit de créer une nouvelle catégorie de signalements et de contribuer ainsi à la mise en œuvre et au suivi de la directive 2008/115/CE[2].

En raison de la géométrie variable de la participation des États membres aux politiques de l'Union européenne en matière de liberté, de sécurité et de justice, il convient d'adopter trois instruments juridiques distincts, qui seront toutefois mis en œuvre de concert pour permettre un bon fonctionnement et une utilisation efficace de l'ensemble du système.

Parallèlement, en vue de consolider et d'améliorer la gestion des informations au niveau de l'Union européenne, la Commission a engagé, en avril 2016, un processus de réflexion sur «[d]es systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité»[3]. L'objectif général est de permettre aux autorités compétentes d'accéder systématiquement aux informations dont elles ont besoin, à partir des différents systèmes d'information à leur disposition. Pour atteindre cet objectif, la Commission a procédé à une analyse de l'architecture des systèmes d'information existants, qui visait à détecter où l'insuffisance des fonctionnalités de ces systèmes et la fragmentation de l'architecture d'ensemble de la gestion des données dans l'Union européenne se traduisent par une information incomplète et déficiente. À l'appui de ce travail, la Commission a constitué un groupe d'experts à haut niveau sur les systèmes d'information et l'interopérabilité, dont les conclusions provisoires ont également inspiré cette première série de propositions pour les questions liées à la qualité des données[4]. Dans son discours sur l'état de l'Union de septembre 2016, le président Juncker a aussi souligné l'importance de remédier aux insuffisances dont souffre actuellement la gestion de l'information et d'améliorer l'interopérabilité et l'interconnexion des systèmes d'information existants.

Une fois que le groupe d'experts à haut niveau sur les systèmes d'information et l'interopérabilité aura remis ses conclusions, attendues au premier semestre 2017, la Commission envisagera, à la mi-2017, une seconde série de propositions visant à améliorer encore l'interopérabilité du SIS avec d'autres systèmes d'information. Le réexamen du règlement (UE) n° 1077/2011[5], portant création de l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), est un volet tout aussi important de ces travaux, qui donnera probablement lieu, lui aussi, à des propositions distinctes de la Commission en 2017. Pour relever les défis actuels en matière de sécurité, il est important d'investir dans un système d'échange et de gestion de l'information rapide, performant et de qualité et d'assurer l'interopérabilité des bases de données et des systèmes d'information de l'UE.

Le cadre législatif régissant actuellement le SIS de deuxième génération – en ce qui concerne son utilisation aux fins des vérifications aux frontières portant sur des ressortissants de pays

---

2 Directive 2008/115/CE du Parlement européen et du Conseil du 16 décembre 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier (JO L 348 du 24.12.2008, p. 98).

3 COM(2016) 205 final du 6.4.2016.

4 Décision 2016/C 257/03 de la Commission du 17.6.2016.

5 Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (JO L 286 du 1.11.2011, p. 1).

tiers – se fonde sur un instrument de l'ancien premier pilier, à savoir le règlement (CE) n° 1987/2006[6]. La présente proposition vise à remplacer[7] cet instrument, afin:

- d'imposer aux États membres l'obligation d'introduire un signalement dans le SIS dans tous les cas où une interdiction d'entrée à l'encontre d'un ressortissant de pays tiers en séjour irrégulier a été prononcée en vertu de dispositions respectant la directive 2008/115/CE;
- d'harmoniser les procédures nationales de consultation du SIS, pour éviter qu'un ressortissant de pays tiers qui fait l'objet d'une interdiction d'entrée ne se voit délivrer un permis de séjour valable par un État membre;
- d'apporter des modifications techniques qui accroissent la sécurité et contribuent à alléger les contraintes administratives;
- de couvrir l'utilisation du SIS de «bout en bout», à savoir non seulement le système central et les systèmes nationaux, mais aussi les besoins des utilisateurs finaux, en garantissant que ces derniers reçoivent toutes les données dont ils ont besoin pour l'exécution de leurs tâches et respectent toutes les règles de sécurité lorsqu'ils traitent des données issues du SIS.

Le train de mesures proposé développe et améliore le système existant, plutôt que d'en créer un nouveau. La révision du SIS, qui soutiendra et renforcera les actions menées par l'Union européenne dans le cadre de l'agenda européen en matière de migration et du programme européen en matière de sécurité, met en œuvre:

(1) les résultats consolidés des travaux sur la mise en œuvre du SIS conduits ces trois dernières années, qui prévoient d'apporter des modifications techniques au SIS central afin d'étendre certaines des catégories de signalements existantes et d'ajouter certaines fonctionnalités;

(2) les recommandations de modifications techniques et procédurales qui ont été formulées à l'issue de l'évaluation complète du SIS[8];

(3) les demandes d'améliorations techniques qui émanaient des utilisateurs finaux du SIS; et

(4) les conclusions provisoires du groupe d'experts à haut niveau sur les systèmes d'information et l'interopérabilité[9] concernant la qualité des données.

La présente proposition étant intrinsèquement liée à la proposition, présentée par la Commission, de règlement sur l'établissement, le fonctionnement et l'utilisation du SIS dans le domaine dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, un certain nombre de dispositions sont communes aux deux textes. Il s'agit notamment: des dispositions relatives à l'utilisation du SIS «de bout en bout», laquelle

---

6 Règlement (CE) n° 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) (JO L 381 du 28.12.2006, p. 4).

7 Voir la section 2 «Choix de l'instrument» pour une explication des raisons ayant motivé le remplacement de la législation en vigueur plutôt qu'une refonte.

8 Rapport d'évaluation du système d'information Schengen de deuxième génération (SIS II) présenté au Parlement européen et au Conseil conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi qu'à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI, et document de travail des services de la Commission l'accompagnant (JO...).

9 Groupe d'experts à haut niveau, rapport du président du 21 décembre 2016.

recouvre non seulement l'exploitation du système central et des systèmes nationaux, mais aussi les besoins des utilisateurs finaux; des dispositions renforcées visant à garantir la continuité des opérations; des dispositions en matière de qualité, de protection et de sécurité des données; et des dispositions en matière de suivi, d'évaluation et de rapports. Les deux propositions prévoient également d'étendre l'utilisation des informations biométriques[10].

Avec l'escalade de la crise des migrants et des réfugiés en 2015, la nécessité de prendre des mesures efficaces pour lutter contre la migration irrégulière s'est considérablement accrue. Dans le *plan d'action de l'UE en matière de retour*[11], la Commission a annoncé qu'elle allait proposer d'obliger les États membres à introduire toutes les interdictions d'entrée dans le SIS afin d'empêcher les ressortissants de pays tiers interdits d'entrée et de séjour sur le territoire des États membres de revenir dans l'espace Schengen. Une interdiction d'entrée prononcée conformément à des dispositions respectant la directive 2008/115/CE s'applique dans tout l'espace Schengen; elle peut donc être mise à exécution à une frontière extérieure par les autorités d'un État membre autre que l'État membre qui l'a décidée. Le règlement (CE) n° 1987/2006 en vigueur se borne à autoriser les États membres à introduire dans le SIS des signalements aux fins de refus d'entrée et de séjour fondés sur une interdiction d'entrée, mais ne l'exige pas d'eux. Le fait de rendre obligatoire la saisie, dans le SIS, de toutes les interdictions d'entrée devrait permettre une plus grande efficacité et une harmonisation plus poussée.

- **Cohérence avec les dispositions en vigueur dans le domaine d'action et les instruments juridiques existants et futurs**

La présente proposition est pleinement alignée et cohérente avec les dispositions de la directive 2008/115/CE (directive sur le retour) relatives à l'imposition et à l'exécution des interdictions d'entrée. Complétant ainsi les dispositions en vigueur en matière d'interdictions d'entrée, le règlement ici proposé contribuera à l'exécution effective de ces interdictions d'entrée aux frontières extérieures, en facilitant l'application des obligations prévues par la directive sur le retour et en empêchant efficacement les ressortissants de pays tiers concernés de revenir dans l'espace Schengen.

- **Cohérence avec les autres politiques de l'Union**

La présente proposition est étroitement liée à d'autres politiques de l'Union, qu'elle complète, à savoir:

(1) la politique de **sécurité intérieure**, puisque le SIS contribuera à empêcher l'entrée des ressortissants de pays tiers qui représentent une menace pour la sécurité;

(2) la politique en matière de **protection des données**, dans la mesure où la présente proposition prévoit de garantir la protection des droits fondamentaux des personnes dont les données à caractère personnel sont traitées dans le SIS.

(3) La présente proposition est aussi étroitement liée à la législation en vigueur de l'Union, qu'elle complète, en ce qui concerne:

(4) la **gestion des frontières extérieures**, dans la mesure où la présente proposition vise à aider les États membres à contrôler leur portion des frontières extérieures de l'Union et, ce faisant, à renforcer l'efficacité du système de contrôles aux frontières extérieures de l'Union;

---

[10] Pour une explication détaillée des modifications prévues dans la présente proposition, voir la section 5 «Autres éléments».

[11] COM(2015) 453 final.

(5) la mise en place d'une **politique de l'Union en matière de retours** qui soit efficace, l'objectif étant de contribuer au système par lequel l'Union détecte et contrecarre les tentatives de rentrée sur son sol de ressortissants de pays tiers ayant fait l'objet d'une mesure de retour, et de le renforcer. La présente proposition vise à contribuer à réduire les incitations à la migration irrégulière vers l'UE, ce qui est l'un des principaux objectifs de l'agenda européen en matière de migration[12];

(6) le **corps européen de garde-frontières et de garde-côtes**, en ce qui concerne: i) la possibilité, pour le personnel de l'Agence européenne de garde-frontières et de garde-côtes, de conduire des analyses de risque; ii) l'accès au SIS de l'unité centrale ETIAS constituée au sein de cette agence, aux fins dudit système européen d'information et d'autorisation concernant les voyages (ETIAS)[13], actuellement en projet; et iii) la mise en place d'une interface technique permettant au corps européen de garde-frontières et de garde-côtes, aux équipes chargées des tâches liées au retour et aux équipes d'appui à la gestion des flux migratoires d'accéder au SIS et d'y consulter des données dans le cadre de leur mandat;

(7) **Europol**, dans la mesure où il est proposé de lui accorder de plus larges droits de consultation du SIS et d'accès aux données qui y sont enregistrées, dans le cadre de son mandat.

La présente proposition est enfin étroitement liée à la législation future de l'Union, qu'elle complètera, en ce qui concerne:

(8) le **système d'entrée/sortie**, puisque la présente proposition vise à tenir compte de l'utilisation combinée d'empreintes digitales et d'images faciales en tant qu'identifiants biométriques qui est envisagée aux fins du bon fonctionnement du système d'entrée/sortie (EES);

(9) l'**ETIAS**, dans le cadre duquel il est proposé de soumettre les ressortissants de pays tiers exemptés de l'obligation de visa qui ont l'intention de se rendre dans l'UE à une évaluation approfondie en matière de sécurité, comprenant notamment une vérification dans le SIS.

## 2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

### • Base juridique

Les dispositions relatives à la gestion intégrée des frontières et à l'immigration clandestine contenues dans la présente proposition sont fondées sur l'article 77, paragraphe 2, points b) et d), et sur l'article 79, paragraphe 2, point c), du traité sur le fonctionnement de l'Union européenne.

### • Géométrie variable

La présente proposition développe les dispositions de l'acquis de Schengen relatives aux vérifications aux frontières. Il y a donc lieu de tenir compte des conséquences liées aux différents protocoles et accords signés avec les pays associés, décrites ci-après.

Danemark: conformément à l'article 4 du protocole n° 22 sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union

[12] COM(2015) 240 final.
[13] COM(2016) 731 final.

européenne, le Danemark décidera, dans un délai de six mois après que le Conseil aura statué sur le présent règlement, s'il met en œuvre celui-ci dans son droit national.

Royaume-Uni et Irlande: conformément aux articles 4 et 5 du protocole n° 19 sur l'acquis de Schengen intégré dans le cadre de l'Union européenne, à la décision 2000/365/CE du Conseil du 29 mai 2000 relative à la demande du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de participer à certaines dispositions de l'acquis de Schengen et à la décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen, le Royaume-Uni et l'Irlande ne participent ni au règlement (UE) 2016/399 (code frontières Schengen), ni à aucun autre des instruments juridiques qui forment ce que l'on appelle l'«acquis de Schengen», à savoir les instruments juridiques organisant et soutenant la suppression des contrôles aux frontières intérieures et les mesures d'accompagnement relatives aux contrôles aux frontières extérieures. Le présent règlement constituant un développement de cet acquis, le Royaume-Uni et l'Irlande ne participent pas à son adoption et ne sont pas liés par celui-ci ni soumis à son application.

Bulgarie et Roumanie: le présent règlement constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte, au sens de l'article 4, paragraphe 2, de l'acte d'adhésion de 2005. Il doit être lu en combinaison avec la décision 2010/365/UE du Conseil du 29 juin 2010[14], qui a rendu applicables en Bulgarie et Roumanie, à certaines restrictions près, les dispositions de l'acquis de Schengen relatives au système d'information Schengen.

Chypre et Croatie: le présent règlement constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte, au sens, respectivement, de l'article 3, paragraphe 2, de l'acte d'adhésion de 2003 et de l'article 4, paragraphe 2, de l'acte d'adhésion de 2011.

Pays associés: sur la base des accords les associant respectivement à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, l'Islande, la Norvège, la Suisse et le Liechtenstein seront liés par le présent règlement.

- **Subsidiarité**

Le règlement proposé se fondera sur le SIS existant, opérationnel depuis 1995, et le développera. Le cadre intergouvernemental initial a été remplacé par des instruments de l'Union le 9 avril 2013 [règlement (CE) n° 1987/2006 et décision 2007/533/JAI du Conseil]. Une analyse de subsidiarité complète a été conduite en de précédentes occasions, et la présente initiative vise à affiner encore les dispositions en vigueur, à combler les lacunes constatées et à améliorer les procédures opérationnelles.

Des solutions décentralisées ne permettraient pas aux États membres d'échanger un volume d'informations aussi considérable. En raison de sa dimension et de ses effets, l'action envisagée peut être mieux réalisée au niveau de l'Union.

La présente proposition a notamment pour objectifs d'apporter des améliorations techniques au SIS pour en accroître l'efficacité et de tendre à harmoniser les modalités d'utilisation du système dans l'ensemble des États membres participants. Compte tenu de la nature transnationale de ces objectifs et du défi consistant à assurer un échange d'informations efficace pour contrer des menaces toujours changeantes, l'Union est bien placée pour proposer des solutions que les seuls États membres ne pourraient suffisamment développer.

---

[14] Décision du Conseil du 29 juin 2010 sur l'application à la République de Bulgarie et à la Roumanie des dispositions de l'acquis de Schengen relatives au système d'information Schengen (JO L 166 du 1.7.2010, p. 17).

Si les limites que présente actuellement le SIS ne sont pas surmontées, son efficacité et la valeur ajoutée de l'Union risquent d'être suboptimales en de nombreuses occasions, et le travail des autorités compétentes risque parfois de se trouver bloqué dans les «angles morts» du système. À titre d'exemple, la libre circulation des personnes, qui est pourtant un principe fondamental de l'Union, peut se trouver entravée du fait de l'absence de règles harmonisées sur la suppression des signalements redondants dans le système.

- **Proportionnalité**

L'article 5 du traité sur l'Union européenne dispose que l'action de l'Union n'excède pas ce qui est nécessaire pour atteindre les objectifs du traité. La forme d'action choisie doit permettre d'atteindre l'objectif de la proposition et de mettre celle-ci en œuvre aussi efficacement que possible. L'initiative ici proposée consiste à réviser le SIS aux fins des vérifications aux frontières.

La proposition est guidée par les principes de respect de la vie privée dès la conception. En termes de protection des données à caractère personnel, le règlement proposé est proportionné, puisqu'il prévoit des règles spécifiques sur la suppression des signalements et ne prescrit pas de collecter plus de données ni de les stocker pendant plus longtemps qu'il n'est absolument nécessaire pour permettre au système de fonctionner et d'atteindre ses objectifs. Les signalements SIS ne contiennent que les données dont les autorités compétentes ont besoin pour identifier et localiser une personne ou un objet et prendre des mesures opérationnelles appropriées. Tout complément est fourni via les bureaux SIRENE, qui permettent l'échange d'informations supplémentaires.

En outre, la proposition prévoit la mise en œuvre de tous les mécanismes et de toutes les garanties nécessaires à la protection effective des droits fondamentaux des personnes concernées, en particulier la protection de leur vie privée et de leurs données à caractère personnel. Elle contient aussi des dispositions spécialement conçues pour renforcer la sécurité des données à caractère personnel conservées dans le SIS.

Aucun processus ni aucune harmonisation supplémentaires ne seront nécessaires au niveau de l'UE pour faire fonctionner le système. La mesure envisagée est donc proportionnée en ce qu'elle n'excède pas ce qui est nécessaire, en termes d'action de l'UE, pour atteindre les objectifs définis.

- **Choix de l'instrument**

La révision proposée prendra la forme d'un règlement remplaçant le règlement (CE) n° 1987/2006. C'est cette approche qui avait été suivie pour la décision 2007/533/JAI du Conseil, et, les deux instruments étant intrinsèquement liés, il convient aussi de la suivre pour le règlement (CE) n° 1987/2006. La décision 2007/533/JAI avait été adoptée en tant qu'instrument dit du «troisième pilier» en vertu de l'ancien traité sur l'Union européenne. Les instruments du «troisième pilier» étaient adoptés par le Conseil sans intervention du Parlement européen comme colégislateur. La présente proposition a pour base juridique le traité sur le fonctionnement de l'Union européenne (TFUE), puisque la structure en piliers a cessé d'exister à l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009. Cette base juridique commande d'appliquer la procédure législative ordinaire. La forme d'un règlement (du Parlement européen et du Conseil) doit être choisie, parce que les dispositions prévues doivent être contraignantes et directement applicables dans tout État membre.

Le règlement proposé développera et améliorera un système centralisé existant par lequel les États membres coopèrent entre eux, ce qui suppose une architecture commune, assortie de

règles de fonctionnement contraignantes. Il prévoit également des règles contraignantes pour l'accès au système, notamment à des fins répressives, qui seront uniformes pour tous les États membres ainsi que pour l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice[15] (eu-LISA). Depuis le 9 mai 2013, l'agence eu-LISA est chargée de la gestion opérationnelle du SIS central, c'est-à-dire de toutes les tâches nécessaires pour assurer le plein fonctionnement du SIS central 24 heures sur 24 et 7 jours sur 7. La présente proposition s'appuie sur les responsabilités liées au SIS qui incombent à l'agence eu-LISA.

La présente proposition prévoit enfin des règles directement applicables, permettant l'accès des personnes concernées à leurs propres données et à des voies de recours, sans que de nouvelles mesures d'exécution ne soient nécessaires à cet égard.

Dès lors, seul un règlement peut être l'instrument juridique retenu.

## 3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

### • Évaluations ex post/bilans de qualité de la législation existante

Conformément au règlement (CE) n° 1987/2006 et à la décision 2007/533/JAI du Conseil[16], trois ans après la mise en service du SIS de deuxième génération, la Commission a procédé à une évaluation complète du système central ainsi que des échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres.

Cette évaluation a tout particulièrement porté sur l'application de l'article 24 du règlement (CE) n° 1987/2006, l'objectif étant d'aboutir aux propositions nécessaires pour modifier cet article de façon à parvenir à un degré plus élevé d'harmonisation des critères selon lesquels les signalements doivent être introduits.

Il est ainsi apparu nécessaire d'apporter des modifications à la base juridique du SIS pour mieux répondre aux nouveaux défis en matière de sécurité et de migration. À ce titre, il est notamment proposé de rendre obligatoires l'introduction dans le SIS des interdictions d'entrée aux fins de leur meilleure exécution et la consultation entre États membres pour empêcher qu'un titre de séjour ne puisse être délivré à une personne frappée d'interdiction d'entrée, d'offrir la possibilité d'identifier et de localiser les personnes sur la base de leurs empreintes digitales grâce à un nouveau système de reconnaissance automatisée d'empreintes digitales et d'étendre la gamme des identifiants biométriques disponibles dans le système.

L'évaluation a également montré la nécessité de modifications juridiques pour améliorer le fonctionnement technique du système et harmoniser les processus nationaux. Ces mesures accroîtront l'efficacité et l'efficience du SIS en en rendant l'utilisation plus facile et en supprimant des contraintes inutiles. D'autres mesures visent à accroître la qualité des données et la transparence du système, par une définition plus claire des obligations spécifiques de rapport incombant aux États membres et à l'agence eu-LISA.

---

15 Instituée par le règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (JO L 286 du 1.11.2011, p. 1).

16 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) (JO L 205 du 7.8.2007, p. 63).

Les résultats de l'évaluation complète (le rapport d'évaluation et le document de travail des services de la Commission qui lui était lié ont été adoptés le 21 décembre 2016[17]) sont à la base des mesures contenues dans la présente proposition.

En outre, conformément à l'article 19 de la directive 2008/115/CE (directive sur le retour), la Commission a publié en 2014 une communication sur la politique de l'Union européenne en matière de retour[18], qui rend compte de l'application de cette directive. Selon les conclusions de cette communication, le potentiel du SIS dans le domaine de la politique de retour devrait être renforcé, et le réexamen du SIS II serait l'occasion d'améliorer la cohérence entre la politique de retour et le SIS II. La Commission suggérait en outre d'instaurer l'obligation, pour les États membres, d'introduire dans le SIS II un signalement aux fins de refus d'entrée pour chaque interdiction d'entrée prononcée en vertu de la directive sur le retour.

- **Consultation des parties intéressées**

Durant l'évaluation du SIS par la Commission, les parties intéressées, y compris les délégués au comité SIS-VIS conformément à la procédure instituée par l'article 51 du règlement (CE) n° 1987/2006, ont été invitées à fournir un retour d'information et à formuler des suggestions. Le comité SIS-VIS est composé de représentants des États membres, à la fois pour les questions opérationnelles SIRENE (coopération transfrontière en relation avec le SIS) et les questions techniques relatives au développement et à la maintenance du SIS et de l'application SIRENE liée.

Dans le cadre de l'évaluation, les délégués ont répondu à des questionnaires détaillés. Lorsque des précisions étaient nécessaires, ou qu'un sujet méritait d'être développé, des échanges par courriel ou des entretiens ciblés ont été utilisés.

Ce processus itératif a permis de traiter les questions en profondeur et dans la transparence. Tout au long de 2015 et de 2016, les délégués au comité SIS-VIS ont discuté dans le cadre de réunions et d'ateliers ad hoc.

En matière de protection des données, la Commission a, en outre, consulté spécifiquement les autorités nationales compétentes et les membres du groupe de coordination des contrôles du SIS II. Les États membres ont partagé leur expérience des demandes d'accès des personnes concernées et du travail des autorités nationales chargées de la protection des données en répondant à un questionnaire ad hoc. L'élaboration de la présente proposition s'est nourrie des réponses à ce questionnaire de juin 2015.

En interne, la Commission a institué un groupe de pilotage interservices, associant le Secrétariat général et les directions générales de la migration et des affaires intérieures, de la justice et des consommateurs, des ressources humaines et de la sécurité, et de l'informatique. Ce groupe de pilotage a suivi le processus d'évaluation et émis des orientations lorsque cela était nécessaire.

L'évaluation a tenu également compte d'éléments factuels recueillis lors de visites d'évaluation sur site dans les États membres, qui visaient à examiner en détail comment le SIS est concrètement utilisé. Des discussions et des entretiens avec des acteurs de terrain et

---

17 Rapport d'évaluation du système d'information Schengen de deuxième génération (SIS II) présenté au Parlement européen et au Conseil conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi qu'à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI, et document de travail des services de la Commission l'accompagnant.

18 COM(2014) 199 final.

des membres des bureaux SIRENE et des autorités nationales compétentes ont eu lieu dans ce cadre.

Les autorités compétentes des États membres en matière de retour ont aussi été invitées à formuler des suggestions et à fournir un retour d'information (notamment sur les effets d'une possible obligation d'introduire un signalement dans le SIS pour toute interdiction d'entrée prononcée en vertu de la directive 2008/115/CE) dans le cadre du groupe de contact de la Commission sur la directive sur le retour, lors des réunions tenues par celui-ci les 16 novembre 2015, 18 mars 2016 et 20 juin 2016.

C'est à la lumière des contributions reçues que la présente proposition prévoit des mesures pour améliorer l'efficience et l'efficacité technique et opérationnelle du système.

- **Obtention et utilisation d'expertise**

Outre la consultation des parties intéressées, la Commission a recherché une expertise externe en commandant quatre études, dont les résultats ont été pris en considération dans l'élaboration de la présente proposition:

- une évaluation technique du SIS (Kurt Salmon)[19]

Cette évaluation a permis de recenser les principaux problèmes de fonctionnement du SIS et les besoins futurs auxquels il conviendrait de répondre, la première préoccupation étant d'assurer une continuité maximale des opérations et l'adaptabilité de la structure globale à des exigences de capacité croissantes;

- une analyse de l'impact, en termes de technologies de l'information et de la communication, de possibles améliorations de l'architecture du SIS II (Kurt Salmon)[20]

Cette étude a analysé le coût actuel de l'exploitation du SIS au niveau national et évalué deux scénarios techniques possibles pour améliorer le système. Ces scénarios contiennent tous deux un ensemble de propositions techniques axées sur l'amélioration du système central et de l'architecture globale;

- une analyse de l'impact, en termes de technologies de l'information et de la communication, des améliorations techniques à apporter à l'architecture du SIS II, rapport final du 10 novembre 2016 (Wavestone)[21]

Cette étude a évalué le coût qu'entraînerait, pour les États membres, la mise en œuvre d'une copie nationale du SIS, sur la base de trois scénarios (un système entièrement centralisé, la mise en œuvre de N.SIS standard, développés et fournis aux États membres par l'agence eu-LISA, et la mise en œuvre de N.SIS distincts, obéissant toutefois à des normes techniques communes).

- une étude sur la faisabilité et les implications de la mise en place, dans le cadre du système d'information Schengen, d'un système permettant d'échanger des

---

19 Commission européenne, rapport final, *SIS II technical assessment*.

20 Commission européenne, rapport final, *ICT Impact Assessment of Possible Improvements to the SIS II Architecture 2016*.

21 Commission européenne, rapport final, *ICT Impact Assessment of the technical improvements to the SIS II architecture*, 10 novembre 2016 (Wavestone).

informations et de contrôler le respect des décisions de retour à l'échelle de l'UE (PwC)[22].

Cette étude a évalué la faisabilité et les implications techniques et opérationnelles des modifications qu'il est proposé d'apporter au SIS en vue de le rendre plus utilisable aux fins du retour des migrants en situation irrégulière et de la prévention de leur rentrée sur le territoire des États membres.

- **Analyse d'impact**

La Commission n'a pas réalisé d'analyse d'impact.

L'impact des modifications qu'il est prévu d'apporter au système a été considéré dans une perspective technique, sur la base des quatre études indépendantes susmentionnées. Depuis 2013, c'est-à-dire depuis que le SIS II a été mis en service le 9 avril 2013 et que la décision 2007/533/JAI est devenue applicable, la Commission a en outre procédé à deux révisions du manuel SIRENE, dont une révision à mi-parcours, qui a débouché sur le lancement d'un nouveau manuel SIRENE[23] le 29 janvier 2015. La Commission a également adopté un catalogue de recommandations et de meilleures pratiques[24]. Par ailleurs, l'agence eu-LISA et les États membres apportent des améliorations techniques itératives régulières au système. La Commission considère toutefois que ces options sont à présent épuisées et qu'il convient de modifier plus globalement la base juridique. En effet, améliorer la mise en œuvre et le contrôle de celle-ci ne saurait suffire à garantir la clarté requise en ce qui concerne, par exemple, l'application des systèmes des utilisateurs finaux et les règles en matière de suppression des signalements.

En outre, comme le prescrivaient l'article 24, paragraphe 5, l'article 43, paragraphe 3, et l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi que l'article 59, paragraphe 3, et l'article 66, paragraphe 5, de la décision 2007/533/JAI, la Commission a procédé à une évaluation complète du SIS et publié un document de travail de ses services en lien avec celle-ci. Les résultats de l'évaluation complète (le rapport d'évaluation et le document de travail des services de la Commission qui lui était lié ont été adoptés le 21 décembre 2016) sont à la base des mesures contenues dans la présente proposition.

Le mécanisme d'évaluation de Schengen prévu dans le règlement (UE) n° 1053/2013[25] permet de procéder à des évaluations juridiques et opérationnelles régulières du fonctionnement du SIS dans les États membres. Ces évaluations sont réalisées conjointement par la Commission et les États membres. Par ce mécanisme, le Conseil adresse aux différents États membres des recommandations fondées sur les évaluations, qui sont conduites dans le cadre de programmes annuels et pluriannuels. Du fait de leur nature individuelle, ces

---

22 *Study on the feasibility and implications of setting up within the framework of the SIS and EU-wide system for exchanging data on and monitoring compliance with return decisions*, 4 avril 2015, PwC.

23 Décision d'exécution (UE) 2015/219 de la Commission du 29 janvier 2015 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) (JO L 44 du 18.2.2015, p. 75).

24 Recommandation de la Commission établissant un catalogue de recommandations et de meilleures pratiques pour une application correcte du système d'information Schengen de deuxième génération (SIS II) et pour l'échange d'informations supplémentaires par les autorités compétentes des États membres mettant en œuvre et utilisant le SIS II [C(2015)9169/1].

25 Règlement (UE) n° 1053/2013 du Conseil du 7 octobre 2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen et abrogeant la décision du comité exécutif du 16 septembre 1998 concernant la création d'une commission permanente d'évaluation et d'application de Schengen (JO L 295 du 6.11.2013, p. 27).

recommandations ne peuvent toutefois se substituer à des règles juridiquement contraignantes, simultanément applicables à tous les États membres qui utilisent le SIS.

Le comité SIS-VIS discute régulièrement de questions opérationnelles et techniques pratiques. Mais même si les réunions du comité favorisent la coopération entre la Commission et les États, le résultat des discussions (faute de modifications législatives) ne suffit pas à remédier aux problèmes causés, par exemple, par des pratiques nationales divergentes.

Les modifications proposées dans le présent règlement n'auraient pas d'incidence économique ni environnementale majeure. En revanche, elles devraient avoir une incidence positive importante sur le plan social, puisqu'elles devraient garantir une sécurité accrue, en permettant d'identifier plus efficacement les personnes qui utilisent une fausse identité, les auteurs d'une infraction grave dont l'identité demeure inconnue après leur geste et les migrants en situation irrégulière qui tirent avantage de l'espace sans contrôles aux frontières intérieures. L'incidence de ces modifications sur les droits fondamentaux et la protection des données a été examinée et elle est exposée de façon plus détaillée dans la section suivante («Droits fondamentaux»).

L'élaboration de la proposition s'est nourrie du vaste ensemble d'éléments factuels recueillis aux fins de l'évaluation globale du SIS de deuxième génération, qui a étudié le fonctionnement du système et les champs d'amélioration possibles. Une étude d'analyse des coûts a également été réalisée, pour s'assurer que l'architecture nationale choisie était la plus appropriée et proportionnée.

- **Droits fondamentaux et protection des données**

La présente proposition développe et améliore un système existant, plutôt que d'en créer un nouveau, et s'appuie de ce fait sur des garanties effectives importantes déjà en place. Cependant, comme le système continuera à traiter des données à caractère personnel et traitera aussi de nouvelles catégories de données biométriques sensibles, il y a des incidences potentielles sur les droits fondamentaux des personnes. Ces incidences ont été dûment prises en considération, et des garanties supplémentaires sont mises en place pour limiter la collecte et le traitement des données à ce qui est strictement nécessaire sur le plan opérationnel et pour restreindre l'accès à ces données aux personnes qui en ont opérationnellement besoin. La présente proposition prévoit des dispositions claires en matière de durée de conservation des données, et le droit des personnes d'accéder aux données les concernant, de les faire corriger et de demander leur effacement en vertu de leurs droits fondamentaux est expressément reconnu et prévu (voir la section sur la protection et la sécurité des données).

En outre, le règlement proposé renforce les mesures de protection des droits fondamentaux, puisqu'il inscrit dans la législation l'obligation d'effacer les signalements et instaure une évaluation de proportionnalité pour le cas où un signalement devrait être prolongé. Pour éviter le risque de porter préjudice à des personnes innocentes, le règlement proposé soumet l'utilisation d'identifiants biométriques à des garanties solides et étendues.

Il prescrit aussi la sécurité du système «de bout en bout», de façon à assurer une meilleure protection des données qui y sont stockées. En instituant une procédure claire pour la gestion des incidents et en améliorant la continuité des opérations du SIS, le règlement proposé est aussi pleinement conforme à la Charte des droits fondamentaux de l'Union européenne[26], et pas uniquement en ce qui concerne le droit à la protection des données à caractère personnel.

---

[26] Charte des droits fondamentaux de l'Union européenne (2012/C 326/02).

Le développement et l'efficacité continue du SIS contribueront à la sécurité des personnes dans la société.

La proposition prévoit des changements importants en ce qui concerne les identifiants biométriques. Outre les empreintes digitales, les empreintes palmaires devraient également être collectées et stockées si les exigences légales sont remplies. Comme le prévoit l'article 24, des fichiers d'empreintes digitales seront attachés aux signalements SIS alphanumériques. Il devrait être possible à l'avenir de confronter à ces données dactylographiques (empreintes digitales et palmaires) les empreintes trouvées sur le lieu d'une infraction, sous réserve que l'infraction commise puisse être qualifiée d'infraction grave ou terroriste et qu'il soit hautement probable que les empreintes trouvées soient celles de l'auteur de l'infraction. Lorsque les documents d'une personne ne permettent pas d'établir son identité avec certitude, les autorités compétentes devraient comparer ses empreintes digitales avec les empreintes digitales stockées dans le SIS.

La proposition prévoit aussi d'exiger la collecte et le stockage de données complémentaires (telles que les informations contenues dans les documents personnels d'identification), afin de faciliter le travail sur le terrain des agents chargés d'établir l'identité d'une personne.

La proposition prévoit enfin de garantir le droit des personnes concernées à un recours effectif leur permettant de contester toute décision et, en tout état de cause, à un recours effectif devant un tribunal conformément à l'article 47 de la Charte des droits fondamentaux.

## 4. INCIDENCE BUDGÉTAIRE

Le SIS constitue un seul système d'information. En conséquence, les dépenses prévues dans deux des propositions du train de mesures considéré [à savoir, la présente proposition et la proposition de règlement 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] ne devraient pas être considérées comme des montants distincts, mais comme formant un tout. Les incidences budgétaires des modifications nécessaires à la mise en œuvre de ces deux propositions sont exposées dans une seule et même fiche financière législative.

En raison de la nature complémentaire de la troisième proposition (relative au retour des ressortissants de pays tiers en séjour irrégulier), les incidences budgétaires de cette troisième proposition sont traitées séparément, dans une fiche financière distincte qui ne concerne que la création de la catégorie spécifique de signalements qui y est prévue.

D'après une évaluation des différents aspects du travail requis pour faire fonctionner le réseau, de ce qu'implique l'administration du SIS central par l'agence eu-LISA et des développements que les États membres devront effectuer, les deux règlements proposés nécessiteront une enveloppe globale de 64,3 millions d'euros pour la période 2018-2020.

Cette enveloppe couvrira notamment un élargissement de la bande passante TESTA-NG, puisque, selon les deux propositions, le réseau transmettra des fichiers d'empreintes digitales et des images faciales, ce qui suppose une augmentation du débit et de la capacité (9,9 millions d'euros). Elle couvrira aussi les dépenses de personnel et les dépenses opérationnelles exposées par l'agence eu-LISA (17,6 millions d'euros). L'agence eu-LISA a informé la Commission qu'elle prévoyait de recruter trois nouveaux agents contractuels en janvier 2018, afin d'entamer la phase de développement suffisamment tôt pour que les fonctionnalités actualisées du SIS puissent être mises en service en 2020. La présente proposition prévoit d'apporter des modifications techniques au SIS central, afin d'élargir

certaines catégories de signalements existantes et d'ajouter de nouvelles fonctionnalités. La fiche financière jointe à la présente proposition reflète ces modifications.

La Commission a également procédé à une étude d'analyse des coûts, pour évaluer ce que coûteraient les développements au niveau national nécessités par la présente proposition[27]. Le coût estimatif se chiffre à 36,8 millions d'euros et il devrait être couvert par le versement d'une somme forfaitaire aux États membres. Chaque État membre recevra ainsi un montant de 1,2 million d'euros pour moderniser son système national et le rendre conforme aux exigences de la présente proposition, ce qui implique notamment de mettre en place une copie nationale partielle lorsque tel n'est pas encore le cas ou un système de secours.

Une reprogrammation du solde de l'enveloppe «frontières intelligentes» du Fonds pour la sécurité intérieure est planifiée, pour permettre les actualisations et la mise en œuvre des fonctionnalités prévues dans les deux propositions. Le règlement FSI-Frontières[28] est l'instrument financier dans lequel le budget consacré à la mise en œuvre du paquet «frontières intelligentes» a été inclus. Son article 5 prévoit que 791 millions d'euros doivent être consacrés à un programme pour la mise en place de systèmes informatiques permettant la gestion des flux migratoires aux frontières extérieures, dans les conditions énoncées à l'article 15. Sur ces 791 millions d'euros, 480 millions d'euros sont réservés au développement du système d'entrée/sortie et 210 millions d'euros au développement du système européen d'information et d'autorisation concernant les voyages (ETIAS). Le solde servira en partie à couvrir le coût des modifications du SIS prévues dans les deux propositions.

## 5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

L'utilisation du SIS fera l'objet d'un examen et d'un suivi réguliers de la part de la Commission, des États membres et de l'agence eu-LISA, qui s'assureront ainsi que le système continue à fonctionner de manière efficace et efficiente. Pour mettre en œuvre les mesures techniques et opérationnelles décrites dans la proposition, la Commission sera assistée par le comité SIS-VIS.

En outre, l'article 54, paragraphes 7 et 8, du règlement proposé prévoit un processus formel d'examen et d'évaluation réguliers.

Tous les deux ans, l'agence eu-LISA sera tenue de remettre au Parlement européen et au Conseil un rapport sur le fonctionnement technique du SIS et de l'infrastructure de communication sur laquelle il s'appuie, y compris la sécurité offerte, et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres.

De plus, tous les quatre ans, la Commission devra procéder à une évaluation globale du SIS et des échanges d'informations entre les États membres et la présenter au Parlement européen et au Conseil. Dans ce cadre, le Commission:

- examinera les résultats atteints par rapport aux objectifs;

---

[27] Wavestone, *ICT Impact Assessment of the technical improvements to the SIS II architecture* – rapport final, 10 novembre 2016, scénario 3, mise en œuvre de N.SIS II distincts.

[28] Règlement (UE) n° 515/2014 du Parlement européen et du Conseil du 16 avril 2014 portant création, dans le cadre du Fonds pour la sécurité intérieure, de l'instrument de soutien financier dans le domaine des frontières extérieures et des visas (JO L 150 du 20.5.2014, p. 143).

- appréciera si les principes qui sous-tendent le système restent valables;
- analysera comment le règlement est appliqué au système central;
- évaluera la sécurité du système central;
- étudiera les implications pour le fonctionnement futur du système.

L'agence eu-LISA est désormais également chargée de fournir des statistiques journalières, mensuelles et annuelles sur l'utilisation du SIS et d'assurer ainsi un suivi continu du système et de son fonctionnement par rapport aux objectifs.

- **Explication détaillée des dispositions nouvelles contenues dans la proposition**

**Dispositions communes à la présente proposition et à la proposition de règlement 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**

- Dispositions générales (articles 1er à 3)
- Architecture technique et mode de fonctionnement du SIS (articles 4 à 14)
- Responsabilités de l'agence eu-LISA (articles 15 à 18)
- Droit d'accès et conservation des signalements (articles 29, 30, 31, 33 et 34)
- Règles générales en matière de traitement et de protection des données (articles 36 à 53)
- Suivi et statistiques (article 54)

**Utilisation du SIS «de bout en bout»**

Comptant plus de 2 millions d'utilisateurs finaux au sein des autorités compétentes de toute l'Europe, le SIS est un outil d'échange d'informations extrêmement utilisé et efficace. Les deux propositions prévoient des règles qui couvrent le système «de bout en bout», à savoir le SIS central géré par l'agence eu-LISA, les systèmes nationaux et les applications des utilisateurs finaux. Sont ainsi pris en compte non seulement le système central et les systèmes nationaux eux-mêmes, mais aussi les besoins techniques et opérationnels des utilisateurs finaux.

L'article 9, paragraphe 2, précise que les utilisateurs finaux doivent recevoir les données dont ils ont besoin pour s'acquitter de leurs tâches (en particulier, toutes les données nécessaires pour identifier la personne concernée et prendre la mesure qui s'impose). Cet article prévoit également un schéma directeur commun pour la mise en œuvre du SIS par les États membres, qui garantira l'harmonisation de tous les systèmes nationaux. Conformément à l'article 6, chaque État membre doit assurer la disponibilité continue du SIS pour les utilisateurs finaux, l'objectif étant de maximiser les avantages opérationnels en réduisant le risque de temps d'arrêt.

L'article 10, paragraphe 3, étend les règles de sécurité aux activités de traitement de données réalisées par les utilisateurs finaux. L'article 14 fait obligation aux États membres de veiller à ce que le personnel ayant accès au SIS reçoive des formations régulières sur la sécurité des données et les règles en matière de protection des données.

Parce qu'elles prévoient ces mesures, qui fixent des règles et des obligations pour les millions d'utilisateurs finaux en Europe, les deux propositions couvrent plus complètement le fonctionnement du SIS «de bout en bout». Pour que le SIS soit utilisé au maximum de son efficacité, les États membres devraient également veiller à ce que, chaque fois que les utilisateurs finaux ont le droit de consulter une base de données nationale de la police ou des services d'immigration, ils consultent aussi le SIS en parallèle. De cette manière, le SIS pourra remplir son objectif de principale mesure compensatoire dans l'espace sans contrôles aux frontières intérieures, et les États membres pourront mieux tenir compte de la dimension transfrontière de la criminalité et de la mobilité des criminels. Cette consultation parallèle devra rester conforme à l'article 4 de la directive (UE) 2016/680[29].

**Continuité des opérations**

Les propositions prévoient des dispositions renforcées en matière de continuité des opérations, tant pour le niveau national que pour l'agence eu-LISA (articles 4, 6, 7 et 15). Ces dispositions garantiront que le SIS reste fonctionnel et accessible aux agents de terrain, même en cas de problèmes affectant le système.

**Qualité des données**

La présente proposition maintient le principe selon lequel l'État membre propriétaire des données est responsable de l'exactitude des données qu'il saisit dans le SIS (article 39). Il est cependant nécessaire de prévoir un mécanisme central, géré par l'agence eu-LISA, qui permette aux États membres de revoir régulièrement les signalements dans lesquels les champs de données obligatoires pourraient poser des problèmes de qualité. C'est pourquoi l'article 15 habilite l'agence eu-LISA à produire, à intervalles réguliers, des rapports sur la qualité des données à l'intention des États membres. La mise en place d'un registre des rapports statistiques et des rapports sur la qualité des données (article 54) facilitera sans doute cette activité. Ces améliorations font suite aux conclusions provisoires du groupe d'experts à haut niveau sur les systèmes d'information et l'interopérabilité.

**Photographies, images faciales, données dactylographiques et profils ADN**

La possibilité d'effectuer une consultation à l'aide d'empreintes digitales pour identifier une personne est déjà prévue par l'article 22 du règlement (CE) n° 1987/2006 et de la décision 2007/533/JAI du Conseil. Les propositions prévoient de rendre cette consultation obligatoire si l'identité de la personne ne peut être établie avec certitude d'une autre manière. À l'heure actuelle, les images faciales ne peuvent pas servir de base à une consultation, mais ne peuvent être utilisées que pour confirmer une identité à l'issue d'une consultation alphanumérique. Les modifications apportées aux articles 22 et 28 prévoient la possibilité d'interroger le système pour pouvoir identifier une personne à partir d'images faciales, de photographies et d'empreintes palmaires lorsque cela deviendra techniquement faisable. La dactylographie est l'étude scientifique des empreintes digitales comme méthode d'identification. Les experts en dactylographie conviennent que les empreintes palmaires présentent un caractère d'unicité et comportent, tout comme les empreintes digitales, des points de référence permettant des comparaisons précises et concluantes. Les empreintes palmaires peuvent être utilisées de la même manière que les empreintes digitales pour établir l'identité d'une personne. Le relevé

[29] 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 (JO L 119 du 4.5.2016, p. 89).

des empreintes palmaires d'une personne en même temps que ses dix empreintes digitales à plat et ses dix empreintes digitales roulées est une pratique des services de police depuis de nombreuses décennies. Les empreintes palmaires sont essentiellement utilisées pour identifier une personne qui a abîmé l'extrémité de ses doigts, que ce soit volontairement pour qu'on ne puisse pas relever ses empreintes digitales ni l'identifier ou involontairement par accident ou sous l'effet d'un travail manuel lourd. Dans le cadre des discussions sur les règles techniques du système de reconnaissance automatisée d'empreintes digitales du SIS, des États membres ont déclaré avoir ainsi fréquemment réussi à identifier des migrants en situation irrégulière ayant délibérément endommagé l'extrémité de leurs doigts pour ne pas être identifiés. Le relevé des empreintes palmaires par les autorités nationales a ensuite permis de les identifier.

L'utilisation d'images faciales à des fins d'identification garantira une plus grande cohérence entre le SIS, d'une part, et le système d'entrée/sortie proposé pour l'UE, les portiques électroniques et les bornes en libre-service, d'autre part. Cette fonctionnalité ne pourra toutefois être utilisée qu'aux points de franchissement frontalier régulier.

**Accès des autorités au SIS – utilisateurs institutionnels**

Cette sous-section décrit les nouveaux éléments contenus dans la proposition qui concernent les droits d'accès au SIS des agences de l'UE (utilisateurs institutionnels). Les droits d'accès des autorités nationales compétentes n'ont pas été modifiés.

Europol (article 30), l'Agence européenne de garde-frontières et de garde-côtes (y compris ses équipes, les équipes chargées des tâches liées au retour et les équipes d'appui à la gestion des flux migratoires) et l'unité centrale ETIAS au sein de cette agence (articles 31 et 32) ont accès au SIS et aux données SIS dont elles ont besoin. Des garanties appropriées sont prévues pour la protection des données contenues dans le système (les dispositions de l'article 33, notamment, restreignent l'accès de ces agences aux seules données dont elles ont besoin pour s'acquitter de leurs tâches).

Le droit d'accès d'Europol est étendu aux signalements introduits aux fins de refus d'entrée, ce qui lui permettra d'exploiter au mieux le système dans l'exercice de ses missions; de même, de nouvelles dispositions garantiront que l'Agence européenne de garde-frontières et de garde-côtes et ses équipes peuvent accéder au système dans le cadre des différentes opérations conduites au titre de leur mandat d'assistance aux États membres. En outre, la proposition de règlement du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) présentée par la Commission[30] prévoit que l'unité centrale ETIAS de l'Agence européenne de garde-frontières et de garde-côtes procèdera à des consultations du SIS via l'ETIAS pour vérifier si les ressortissants de pays tiers qui demandent une autorisation de voyage ne font pas l'objet d'un signalement dans le SIS. À cet effet, l'unité centrale ETIAS disposera également d'un accès au SIS[31].

L'article 29, paragraphe 3, prévoit pour sa part que les autorités nationales chargées des visas pourront aussi accéder, dans l'exercice de leurs missions, aux signalements de documents qui auront été introduits en vertu du règlement [.../...] 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.

---

30 COM(2016) 731 final.

31 L'unité centrale ETIAS aura accès aux signalements visés aux articles 24 et 27 du présent règlement.

Ces acteurs pourront ainsi accéder aux données contenues dans le SIS dont ils ont besoin pour exercer leurs missions, mais, parallèlement, des garanties appropriées de protection de ces données sont mises en place (et notamment l'article 35, qui restreint le droit d'accès de ces acteurs aux seules données dont ils ont besoin pour exercer leurs missions).

**Refus d'entrée et de séjour**

Dans sa version actuelle, l'article 24, paragraphe 3, du règlement SIS II prévoit qu'un État membre peut introduire un signalement dans le SIS concernant toute personne frappée d'une interdiction d'entrée fondée sur le non-respect de la réglementation nationale en matière de migration. Dans sa version révisée, l'article 24, paragraphe 3, imposera l'obligation d'introduire un signalement dans le SIS dans tous les cas où une interdiction d'entrée à l'encontre d'un ressortissant de pays tiers en séjour irrégulier a été prononcée en vertu de dispositions respectant la directive 2008/115/CE. Il fixe également le délai et les modalités selon lesquels un tel signalement doit être introduit une fois que le ressortissant de pays tiers visé a quitté le territoire des États membres en exécution d'une obligation de retour. Cette disposition est insérée pour éviter qu'une interdiction d'entrée ne soit visible dans le SIS alors que le ressortissant de pays tiers concerné est encore présent dans l'UE. Dans la mesure où elles prohibent la rentrée sur le territoire des États membres, les interdictions d'entrée ne peuvent prendre effet qu'après le retour des ressortissants de pays tiers visés. Parallèlement, les États membres devraient prendre toutes les mesures nécessaires pour faire en sorte qu'il n'y ait pas de délai entre le moment du retour et l'activation dans le SIS du signalement introduit aux fins de refus d'entrée et de séjour.

La présente proposition est étroitement liée à la proposition de la Commission[32] relative à l'utilisation du SIS aux fins du retour des ressortissants de pays tiers en séjour irrégulier, qui définit les modalités et procédures d'introduction dans le SIS des signalements concernant des décisions de retour. Cette dernière proposition prévoit un mécanisme pour contrôler si les ressortissants de pays tiers frappés d'une décision de retour quittent effectivement le territoire de l'UE, ainsi qu'un mécanisme d'alerte en cas de non-respect d'une telle décision. L'article 26 définit la procédure de consultation que les États membres devront suivre lorsqu'ils tomberont sur un signalement introduit aux fins de refus d'entrée et de séjour, ou lorsqu'ils souhaiteront introduire un tel signalement, qui va à l'encontre d'une décision d'un autre État membre, par exemple un titre de séjour en cours de validité. Les règles définies devraient empêcher l'apparition d'instructions contradictoires auxquelles ces situations pourraient donner lieu, ou permettre de résoudre ces contradictions, tout en offrant des orientations claires permettant aux utilisateurs finaux de savoir quelle est la conduite à tenir dans de telles situations et aux États membres de déterminer s'il convient de supprimer un signalement.

L'article 27 [correspondant à l'ex-article 26 du règlement (CE) n° 1987/2006] vise à mettre en œuvre le régime de sanctions de l'UE applicable aux ressortissants de pays tiers soumis à une mesure de restriction à l'admission sur le territoire de l'UE conformément à l'article 29 du traité sur l'Union européenne. Afin de permettre l'introduction des signalements correspondants, il fallait exiger les données minimales nécessaires à l'identification de la personne, à savoir son nom et sa date de naissance. Le fait que le règlement (CE) n° 1987/2006 dispensait de l'obligation d'indiquer la date de naissance a créé d'importantes difficultés, puisque, conformément aux règles techniques et aux paramètres de recherche du système, aucun signalement ne peut être introduit dans le SIS sans la date de naissance.

[32] COM(2016)…

L'article 27 étant indispensable à l'efficacité du régime de sanctions de l'UE, l'obligation d'évaluation de la proportionnalité ne s'applique pas ici.

Afin d'assurer une plus grande cohérence avec la directive 2008/115/CE, la terminologie utilisée pour faire référence à la finalité de ces signalements a été alignée sur la formulation utilisée dans cette directive («refus d'entrée et de séjour»).

**Différenciation des personnes présentant des caractéristiques similaires**

Afin de garantir un traitement et un stockage appropriés des données et de réduire le risque de duplication et d'erreur d'identification, l'article 41 fixe la procédure à suivre s'il apparaît, lors de l'introduction d'un nouveau signalement, qu'il existe déjà dans le SIS une entrée présentant des caractéristiques similaires.

**Protection et sécurité des données**

La présente proposition clarifie les responsabilités en matière de prévention, de déclaration et de traitement des incidents susceptibles d'affecter la sécurité ou l'intégrité de l'infrastructure du SIS, des données qui y sont contenues ou des informations supplémentaires (articles 10, 16 et 40).

L'article 12 contient des dispositions sur la tenue de journaux contenant l'historique des signalements et la consultation de ces journaux.

L'article 15, paragraphe 3, maintient l'article 15, paragraphe 3, du règlement (CE) n° 1987/2006. Il prévoit que la Commission reste chargée de la gestion contractuelle de l'infrastructure de communication, et notamment des tâches liées à l'exécution du budget, à l'acquisition et au renouvellement. Ces tâches seront transférées à l'agence eu-LISA dans le cadre du second train de propositions relatives au SIS, en juin 2017.

L'article 21 étend l'obligation incombant aux États membres d'évaluer la proportionnalité d'un signalement avant de l'introduire en la rendant applicable aux décisions d'extension de la durée de validité d'un signalement Toutefois, l'article 24, paragraphe 2, point c), impose aussi aux États membres l'obligation nouvelle de créer, en toutes circonstances, un signalement sur les personnes dont les activités relèvent de l'article 1er, 2, 3 ou 4 de la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme.

Catégories de données et traitement des données

Afin de permettre une identification plus efficace de la personne signalée et de faciliter et d'accélérer l'exécution de la conduite à tenir, en mettant à la disposition des utilisateurs finaux plus d'informations et des informations plus précises, la présente proposition prévoit d'étendre aux informations suivantes les types d'informations pouvant être détenus sur une telle personne:

- l'indication que la personne est impliquée dans une activité mentionnée aux articles 1er, 2, 3 ou 4 de la décision-cadre 2002/475/JAI du Conseil;
- l'indication que le signalement concerne un citoyen de l'Union ou une autre personne jouissant de droits en matière de libre circulation équivalents à ceux des citoyens de l'Union;
- l'indication que la décision de refus d'entrée est fondée sur les dispositions de l'article 24 ou de l'article 27;

- le type d'infraction (pour les signalements introduits en vertu de l'article 24, paragraphe 2);
- le détail d'un document d'identité ou de voyage de la personne;
- une photocopie couleur de ce document d'identité ou de voyage;
- les photographies et les images faciales;
- les empreintes digitales et les empreintes palmaires.

Pour pouvoir identifier dûment une personne qui est contrôlée à un point de franchissement frontalier, qui fait l'objet d'une vérification à l'intérieur du territoire ou qui sollicite un permis de séjour, il est essentiel de disposer de données appropriées. Une erreur d'identification peut se traduire par une violation des droits fondamentaux de la personne concernée; elle peut également générer une situation dans laquelle les mesures de suivi qui s'imposent ne peuvent pas être prises, faute de savoir qu'un signalement a été introduit ou d'en connaître le contenu.

En ce qui concerne les informations relatives à la décision sous-jacente, la proposition distingue quatre motifs: une précédente condamnation, telle que visée à l'article 24, paragraphe 2, point a); une menace sérieuse pour la sécurité, telle que visée à l'article 24, paragraphe 2, point b); une interdiction d'entrée, telle que visée à l'article 24, paragraphe 3; et une mesure restrictive, telle que visée à l'article 27. Afin de garantir que les mesures appropriées sont prises en cas de réponse positive, il est également nécessaire d'indiquer si le signalement concerne un citoyen de l'Union ou une autre personne jouissant de droits de libre circulation équivalents à ceux des citoyens de l'Union. Pour pouvoir identifier dûment une personne qui est contrôlée à un point de franchissement frontalier, qui fait l'objet d'une vérification à l'intérieur du territoire ou qui sollicite un permis de séjour, il est essentiel de disposer de données appropriées. Une erreur d'identification peut se traduire par une violation des droits fondamentaux de la personne concernée; elle peut également générer une situation dans laquelle les mesures de suivi qui s'imposent ne peuvent être prises, faute de savoir qu'un signalement a été introduit ou d'en connaître le contenu.

L'article 42 étend la liste des données à caractère personnel qui peuvent être introduites et traitées dans le SIS dans les cas d'usurpation d'identité, puisqu'un plus grand volume de données facilitera l'identification de la victime et de l'usurpateur. Cette extension est sans risque, puisque l'ensemble de ces données ne pourra être introduit dans le SIS qu'avec le consentement de la victime dont l'identité a été usurpée. Elles incluent désormais aussi:

- des images faciales;
- des empreintes palmaires;
- le détail de documents d'identité;
- l'adresse de la victime;
- le nom du père et de la mère de la victime.

L'article 20 prévoit l'inclusion d'informations plus détaillées dans les signalements, et notamment les types de motif de refus d'entrée et de séjour et le détail des documents personnels d'identification des personnes concernées. Outre qu'elle permettra une identification plus efficace de la personne concernée, l'introduction d'informations plus détaillées permettra aussi aux utilisateurs finaux de prendre une décision plus éclairée. Aux fins de la protection des utilisateurs finaux qui effectuent les vérifications, le SIS montrera

également si la personne signalée relève de l'une des catégories prévues aux articles 1er, 2, 3 et 4 de la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme[33].

Enfin, la proposition prévoit clairement qu'il est interdit à un État membre de copier dans d'autres fichiers nationaux des données saisies dans le SIS par un autre État membre (article 37).

Conservation des signalements

L'article 34 fixe les délais de réexamen des signalements. La durée de conservation maximale des signalements introduits aux fins de refus d'entrée et de séjour a été alignée sur la durée de validité maximale des interdictions d'entrée prononcées en vertu de l'article 11 de la directive 2008/115/CE. La durée de conservation maximale passera à 5 ans, mais les États membres pourront définir des durées de conservation plus courtes.

Suppression des signalements

L'article 35 prévoit les circonstances dans lesquelles les signalements doivent être supprimés, ce qui permettra une plus grande harmonisation des pratiques nationales en la matière. Il contient des dispositions particulières prévoyant la suppression proactive, par le personnel des bureaux SIRENE, des signalements qui ne sont plus nécessaires si aucune réponse n'est reçue des autorités compétentes.

Droits des personnes concernées à accéder aux données, à faire rectifier les données inexactes et à demander l'effacement des données stockées illégalement

Les règles détaillées relatives aux droits des personnes concernées n'ont pas été modifiées, les dispositions actuelles étant déjà conformes à celles du règlement (UE) 2016/679[34] et de la directive 2016/680[35] et assurant un niveau élevé de protection. En outre, l'article 48 fixe les conditions dans lesquelles les États membres peuvent décider de ne pas communiquer des informations aux personnes concernées. Une telle décision doit impérativement être motivée par l'une des raisons énumérées dans cet article et doit être à la fois nécessaire et proportionnée, conformément au droit national.

Statistiques

Afin de conserver une vue d'ensemble du fonctionnement des recours, l'article 49 définit les modalités d'un système statistique normalisé fournissant des comptes rendus annuels sur:

- le nombre de demandes d'accès présentées par des personnes concernées;
- le nombre de demandes de rectification de données inexactes et d'effacement de données stockées illégalement;

---

33 Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

34 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) (JO L 119 du 4.5.2016, p. 1).

35 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 (JO L 119 du 4.5.2016, p. 89).

- le nombre d'affaires portées devant les tribunaux;
- le nombre d'affaires dans lesquelles la juridiction saisie s'est prononcée en faveur du demandeur; et
- les observations relatives aux cas de reconnaissance mutuelle de décisions définitives rendues par les juridictions ou les autorités d'États membres concernant des signalements d'un État membre signalant.

**Suivi et statistiques**

L'article 54 arrête les dispositions qui doivent être mises en place pour assurer un suivi adéquat du SIS et de son fonctionnement eu égard à ses objectifs. Pour ce faire, l'agence eu-LISA est chargée de fournir des statistiques journalières, mensuelles et annuelles sur la manière dont le système est utilisé.

L'article 54, paragraphe 5, impose à l'agence eu-LISA de fournir aux États membres, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes les rapports statistiques qu'elle produit, et autorise la Commission à demander d'autres rapports statistiques et d'autres rapports sur la qualité des données en lien avec le SIS et la communication SIRENE.

L'article 54, paragraphe 6, prévoit la création et l'hébergement d'un registre central de données dans le cadre du travail de suivi du fonctionnement du SIS dont est chargée l'agence eu-LISA. Ce registre permettra au personnel dûment autorisé par les États membres, la Commission, Europol et l'Agence européenne de garde-frontières et de garde-côtes d'accéder aux données énumérées à l'article 54, paragraphe 3, afin de produire les statistiques requises.

2016/0408 (COD)

Proposition de

# RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

## sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant le règlement (UE) n° 515/2014 et abrogeant le règlement (CE) n° 1987/2006

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 77, paragraphe 2, points b) et d), et son article 79, paragraphe 2, point c),

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Le système d'information Schengen (le «SIS») constitue un outil essentiel pour l'application des dispositions de l'acquis de Schengen, intégré dans le cadre de l'Union européenne. Il représente l'une des grandes mesures compensatoires qui contribuent au maintien d'un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne par le soutien qu'il apporte à la coopération opérationnelle en matière pénale entre les garde-frontières, la police, les douanes, les autres autorités répressives, les autorités judiciaires et les services de l'immigration.

(2) Le SIS a été créé conformément aux dispositions du titre IV de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États 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[36] (la «convention de Schengen»), signée le 19 juin 1990. La Commission a été chargée du développement du SIS de deuxième génération (le «SIS II») par le règlement (CE) n° 2424/2001 du Conseil[37] et la décision 2001/886/JAI du Conseil[38] et

---

[36] JO L 239 du 22.9.2000, p. 19. Convention modifiée en dernier lieu par le règlement (CE) n° 1160/2005 du Parlement européen et du Conseil (JO L 191 du 22.7.2005, p. 18).

[37] JO L 328 du 13.12.2001, p. 4.

[38] Décision 2001/886/JAI du Conseil du 6 décembre 2001 relative au développement du système d'information de Schengen de deuxième génération (SIS II) (JO L 328 du 13.12.2001, p. 1).

le SIS II a été créé par le règlement (CE) n° 1987/2006[39] et la décision 2007/533/JAI du Conseil[40]. Le SIS II a remplacé le SIS tel que créé par la convention de Schengen.

(3) Trois ans après l'entrée en service du SIS II, la Commission a procédé à une évaluation du système, comme le prescrivaient l'article 24, paragraphe 5, l'article 43, paragraphe 5, et l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi que l'article 59 et l'article 65, paragraphe 5, de la décision 2007/533/JAI. Le rapport d'évaluation et le document de travail des services de la Commission qui lui était lié ont été adoptés le 21 décembre 2016[41]. Il convient de tenir compte des recommandations formulées dans ces documents, s'il y a lieu, dans le présent règlement.

(4) Le présent règlement constitue la base législative requise pour régir le SIS dans les domaines relevant du titre V, chapitre 2, du traité sur le fonctionnement de l'Union européenne. Le règlement (UE) 2018/... du Parlement européen et du Conseil 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[42] constitue la base législative requise pour régir le SIS dans les domaines relevant du champ d'application du titre V, chapitres 4 et 5, du traité sur le fonctionnement de l'Union européenne.

(5) Le fait que la base législative requise pour régir le SIS consiste en des instruments distincts n'affecte pas le principe selon lequel le SIS constitue un système d'information unique qui devrait fonctionner en tant que tel. Certaines dispositions de ces instruments devraient donc être identiques.

(6) Il est nécessaire de préciser les objectifs du SIS, son architecture technique et son financement, de fixer des règles concernant son fonctionnement et son utilisation «de bout en bout» et de définir les responsabilités y afférentes, ainsi que les catégories de données à introduire dans le système, les finalités et les critères de leur introduction, les autorités qui sont autorisées à y avoir accès, l'utilisation d'identifiants biométriques, et d'autres règles relatives au traitement des données.

(7) Le SIS comprend un système central (SIS central) et des systèmes nationaux qui comportent une copie intégrale ou partielle de la base de données du SIS. Étant donné qu'il est l'instrument d'échange d'informations le plus important en Europe, il est indispensable de garantir son fonctionnement ininterrompu au niveau tant central que national. C'est pourquoi chaque État membre devrait créer une copie partielle ou intégrale de la base de données du SIS et mettre en place son système de secours.

(8) Il est nécessaire de disposer d'un manuel qui contienne des règles détaillées sur l'échange d'informations supplémentaires concernant la conduite à tenir à la suite de signalements. Des autorités nationales de chaque État membre (bureaux SIRENE) devraient assurer cet échange d'informations.

---

39 Règlement (CE) n° 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) (JO L 381 du 28.12.2006, p. 4).

40 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) (JO L 205 du 7.8.2007, p. 63).

41 Rapport d'évaluation du système d'information Schengen de deuxième génération (SIS II) présenté au Parlement européen et au Conseil conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi qu'à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI, et document de travail des services de la Commission l'accompagnant.

42 Règlement (UE) 2018/…

(9) En vue de l'échange efficace d'informations supplémentaires concernant la conduite à tenir mentionnée dans les signalements, il y a lieu de renforcer le fonctionnement des bureaux SIRENE en précisant les besoins en matière de ressources disponibles, de formation des utilisateurs et de délai de réponse aux demandes de renseignements reçues d'autres bureaux SIRENE.

(10) L'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice[43] (l'«agence eu-LISA») est chargée de la gestion opérationnelle des éléments centraux du SIS. Afin de permettre à l'agence eu-LISA de consacrer les moyens financiers et humains nécessaires pour couvrir tous les aspects de la gestion opérationnelle du SIS central, le présent règlement devrait décrire ses tâches en détail, notamment pour les aspects techniques de l'échange d'informations supplémentaires.

(11) Sans préjudice de la responsabilité des États membres relative à l'exactitude des données introduites dans le SIS, l'agence eu-LISA devrait être chargée de renforcer la qualité des données, en introduisant un outil de contrôle central de cette qualité, et de présenter des rapports réguliers aux États membres.

(12) En vue d'un meilleur contrôle de l'utilisation du SIS pour analyser les tendances en matière de pression migratoire et de gestion des frontières, l'agence eu-LISA devrait être en mesure d'acquérir la capacité de fournir, en utilisant les méthodes les plus modernes, des rapports statistiques aux États membres, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes sans compromettre l'intégrité des données. Il conviendrait dès lors de créer un fichier statistique central. Les statistiques produites ne devraient pas contenir de données à caractère personnel.

(13) Le SIS devrait contenir d'autres catégories de données pour permettre aux utilisateurs finaux de prendre des décisions éclairées fondées sur un signalement sans perdre de temps. En conséquence, les signalements aux fins de refus d'entrée et de séjour devraient comprendre des informations concernant la décision sur laquelle le signalement est fondé. En outre, afin de faciliter l'identification et de détecter les identités multiples, le signalement devrait comporter une référence au document ou numéro d'identification personnel et une copie de ce document, si elle est disponible.

(14) Le SIS ne devrait pas stocker de données ayant servi à des consultations, sauf les journaux conservés afin de pouvoir contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS, ainsi que l'intégrité et la sécurité des données.

(15) Le SIS devrait permettre le traitement des données biométriques afin d'aider à l'identification correcte des personnes concernées. À cet égard, le SIS devrait également permettre le traitement de données relatives à des personnes dont l'identité a été usurpée (de manière à éviter les problèmes que pourraient causer des erreurs d'identification), sous réserve de garanties adaptées, en particulier le consentement des personnes concernées et une stricte limitation des fins auxquelles ces données peuvent être licitement traitées.

(16) Les États membres devraient prendre les mesures techniques nécessaires pour que, chaque fois que les utilisateurs finaux ont le droit de consulter une base de données nationale des services de police ou d'immigration, ils puissent aussi consulter le SIS

---

[43] Instituée par le règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (JO L 286 du 1.11.2011, p. 1).

en parallèle, conformément à l'article 4 de la directive (UE) 2016/680 du Parlement européen et du Conseil[44]. Le SIS serait ainsi la principale mesure compensatoire dans l'espace sans contrôles aux frontières intérieures et tiendrait mieux compte de la dimension transfrontière de la criminalité et de la mobilité des criminels.

(17) Le présent règlement devrait définir les conditions d'utilisation des données dactylographiques et des images faciales à des fins d'identification. Le recours aux images faciales pour identifier des personnes dans le SIS devrait en outre assurer la cohérence des procédures de contrôle aux frontières dans lesquelles l'identification et la vérification de l'identité doivent être réalisées à l'aide des données dactylographiques et des images faciales. Une consultation à l'aide des données dactylographiques devrait être obligatoire s'il y a le moindre doute sur l'identité d'une personne. L'identification par image faciale ne devrait avoir lieu que dans le contexte des contrôles aux frontières réguliers, aux bornes en libre service et aux portiques électroniques.

(18) Les empreintes digitales trouvées sur le lieu d'une infraction devraient pouvoir être comparées aux données dactylographiques stockées dans le SIS s'il peut être établi avec un degré élevé de probabilité qu'elles sont celles de l'auteur de l'infraction grave ou de l'infraction terroriste. Les «infractions graves» devraient correspondre aux infractions énumérées dans la décision-cadre 2002/584/JAI du Conseil[45] et les «infractions terroristes» aux infractions définies par le droit national visées dans la décision-cadre 2002/475/JAI du Conseil[46].

(19) Il devrait être possible pour les États membres de mettre en relation les signalements dans le SIS. Cette mise en relation par un État membre de deux signalements ou plus ne devrait avoir aucun effet sur la conduite à tenir, la durée de conservation ou les droits d'accès aux signalements.

(20) Un niveau accru d'efficacité, d'harmonisation et de cohérence peut être atteint si l'on rend obligatoire l'introduction dans le SIS de toutes les interdictions d'entrée prononcées par les autorités compétentes des États membres conformément à des procédures respectant la directive 2008/115/CE[47], et si l'on établit des règles communes pour l'introduction de tels signalements à la suite du retour du ressortissant de pays tiers en séjour irrégulier. Les États membres devraient prendre toutes les mesures nécessaires pour faire en sorte qu'il n'y ait pas de délai entre le moment où le ressortissant de pays tiers quitte l'espace Schengen et l'activation du signalement dans le SIS. Cela devrait garantir l'application efficace des interdictions d'entrée aux points de passage des frontières extérieures, en empêchant effectivement toute nouvelle entrée dans l'espace Schengen.

---

44 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 (JO L 119 du 4.5.2016, p. 89).

45 Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

46 Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

47 Directive 2008/115/CE du Parlement européen et du Conseil du 16 décembre 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier (JO L 348 du 24.12.2008, p. 98).

(21) Le présent règlement devrait établir des règles obligatoires prévoyant la consultation des autorités nationales lorsqu'un ressortissant de pays tiers est titulaire d'un titre de séjour valable, d'une autre autorisation ou d'un droit de séjour accordé dans un État membre, ou pourrait obtenir un titre, une autorisation ou un droit de ce type, et qu'un autre État membre a déjà introduit ou envisage d'introduire un signalement aux fins de refus d'entrée et de séjour du ressortissant de pays tiers concerné. De telles situations créent en effet de graves incertitudes pour les garde-frontières, la police et les services de l'immigration. Par conséquent, il convient de prévoir un délai impératif pour procéder à une consultation rapide et obtenir un résultat définitif, afin d'éviter que des personnes qui constituent une menace puissent entrer dans l'espace Schengen.

(22) Le présent règlement devrait s'appliquer sans préjudice de l'application de la directive 2004/38/CE[48].

(23) Les signalements ne devraient pas être conservés dans le SIS pour une durée plus longue que le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits. Afin de réduire la charge administrative des différentes autorités qui traiteront des données relatives aux personnes pour différentes finalités, il y a lieu d'aligner la durée maximale de conservation des signalements aux fins de refus d'entrée et de séjour sur la durée maximale possible des interdictions d'entrée prononcées conformément à des procédures respectant la directive 2008/115/CE. En conséquence, la durée de conservation des signalements de personnes devrait être de cinq ans au maximum. À titre de principe général, les signalements de personnes devraient être automatiquement supprimés du SIS après cinq ans. La décision de conserver des signalements de personnes devrait être fondée sur une évaluation individuelle complète. Les États membres devraient réexaminer les signalements de personnes dans le délai défini et tenir des statistiques concernant le nombre de signalements de personnes dont la durée de conservation a été prolongée.

(24) L'introduction et la prorogation de la date d'expiration d'un signalement dans le SIS devraient être soumises à l'obligation de proportionnalité, en vérifiant si un cas déterminé est suffisamment approprié, pertinent et important pour justifier l'introduction d'un signalement dans le SIS. Dans le cas des infractions décrites aux articles 1er, 2, 3 ou 4 de la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme[49], un signalement aux fins de refus d'entrée et de séjour devrait toujours être créé en ce qui concerne les ressortissants de pays tiers concernés, compte tenu du niveau élevé de menace et de l'incidence négative globale que de telles activités peuvent avoir.

(25) L'intégrité des données du SIS est de la plus haute importance. Il convient dès lors de prévoir des mesures de protection adaptées pour que les données du SIS soient traitées, au niveau tant central que national, d'une manière qui assure leur sécurité de bout en bout. Les autorités intervenant dans le traitement des données devraient être liées par les obligations de sécurité imposées par le présent règlement et soumises à une procédure uniforme de déclaration des incidents.

---

48 Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres (JO L 158 du 30.4.2004, p. 77).

49 Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

(26) Les données traitées dans le SIS en application du présent règlement ne devraient pas être transférées à des pays tiers ou à des organisations internationales ni mises à leur disposition.

(27) Afin de renforcer l'efficacité du travail des services de l'immigration lorsqu'ils statuent sur le droit d'entrée et de séjour de ressortissants de pays tiers sur le territoire des États membres, ainsi que sur le retour de ressortissants de pays tiers en séjour irrégulier, il convient de leur donner un accès au SIS en vertu du présent règlement.

(28) Le règlement (UE) 2016/679[50] devrait s'appliquer aux traitements de données à caractère personnel effectués en vertu du présent règlement par les autorités des États membres lorsque la directive (UE) 2016/680[51] ne s'applique pas. Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil[52] devrait s'appliquer aux traitements de données à caractère personnel effectués par les institutions et organes de l'Union dans l'exercice de leurs fonctions en vertu du présent règlement. Il convient de préciser davantage dans le présent règlement, lorsque c'est nécessaire, les dispositions de la directive (UE) 2016/680, du règlement (UE) 2016/679 et du règlement (CE) n° 45/2001. En ce qui concerne le traitement de données à caractère personnel par Europol, le règlement (UE) 2016/794 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs[53] («règlement Europol») est d'application.

(29) En ce qui concerne la confidentialité, les dispositions pertinentes du statut des fonctionnaires et du régime applicable aux autres agents de l'Union européenne devraient s'appliquer aux fonctionnaires et autres agents employés et travaillant en liaison avec le SIS.

(30) Tant les États membres que l'agence eu-LISA devraient disposer de plans de sécurité visant à faciliter la mise en œuvre des obligations en matière de sécurité, ainsi que coopérer de manière à traiter les questions de sécurité dans une perspective commune.

(31) Les autorités de contrôle indépendantes nationales devraient vérifier la licéité des traitements de données à caractère personnel effectués par les États membres dans le cadre du présent règlement. Le droit d'accès, de rectification et d'effacement de leurs données à caractère personnel stockées dans le SIS dont bénéficient les personnes concernées, ainsi que les recours juridictionnels ultérieurs et la reconnaissance mutuelle des décisions judiciaires, devraient être précisés. Il y a donc lieu d'imposer aux États membres de communiquer des statistiques annuelles.

---

50 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) (JO L 119 du 4.5.2016, p. 1).

51 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 (JO L 119 du 4.5.2016, p. 89).

52 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

53 Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 25.5.2016, p. 53).

(32) Les autorités de contrôle devraient veiller à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données dans leur N.SIS, répondant aux normes internationales en matière d'audit. Cet audit devrait être réalisé par les autorités de contrôle elles-mêmes ou être commandé directement par elles à un auditeur indépendant en matière de protection des données. Ce dernier devrait rester sous le contrôle et la responsabilité de la ou des autorités de contrôle nationales, qui devraient donc commander l'audit proprement dit et définir clairement son objet, son étendue et sa méthode, et donner des indications et des instructions sur l'audit et ses résultats finaux.

(33) Le règlement (UE) 2016/794 («règlement Europol») prévoit qu'Europol soutient et renforce l'action des autorités compétentes des États membres et leur coopération mutuelle dans la prévention du terrorisme et des formes graves de criminalité et qu'il fournit des analyses et des évaluations de la menace. Afin de faciliter l'accomplissement des missions d'Europol, en particulier au sein du Centre européen chargé de lutter contre le trafic de migrants, il convient de permettre à Europol d'accéder aux catégories de signalements définies dans le présent règlement. Puisque le Centre européen chargé de lutter contre le trafic de migrants, créé au sein d'Europol, joue un rôle stratégique majeur dans la lutte contre les filières d'immigration irrégulière, il devrait obtenir l'accès aux signalements de personnes auxquelles l'entrée et le séjour sur le territoire d'un État membre sont refusés pour des motifs de nature pénale ou pour non-respect des conditions d'entrée ou de séjour.

(34) Afin de pallier le partage insuffisant d'informations sur le terrorisme, en particulier sur les combattants terroristes étrangers, dont la surveillance des mouvements est essentielle, les États membres devraient partager avec Europol leurs informations sur les activités liées au terrorisme, parallèlement à l'introduction de signalements dans le SIS, ainsi que les réponses positives et les informations y afférentes. Le Centre européen de la lutte contre le terrorisme, créé au sein d'Europol, pourrait ainsi vérifier s'il existe des informations contextuelles supplémentaires dans les bases de données d'Europol et produire des analyses de grande qualité qui aideraient à démanteler les réseaux terroristes et, si possible, à les empêcher de commettre des attentats.

(35) Il est également nécessaire d'établir des règles précises au sujet du traitement et du téléchargement par Europol des données du SIS, pour permettre l'utilisation la plus complète du système, à condition que les normes de protection des données soient respectées comme le prévoient le présent règlement et le règlement (UE) 2016/794. Lorsqu'il ressort d'une consultation du SIS par Europol qu'il existe un signalement introduit par un État membre, Europol ne peut pas exécuter la conduite à tenir requise. Il devrait dès lors informer l'État membre concerné pour lui permettre de donner suite à l'affaire.

(36) Le règlement (UE) 2016/1624 du Parlement européen et du Conseil[54] prévoit, aux fins du présent règlement, que l'État membre hôte autorise les membres des équipes du corps européen de garde-frontières et de garde-côtes ou d'équipes d'agents impliqués dans les tâches liées aux retours, déployées par l'Agence européenne de garde-frontières et de garde-côtes, à consulter les bases de données européennes dont la consultation est nécessaire à la réalisation des objectifs opérationnels spécifiés dans le

[54] Règlement (UE) 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) n° 863/2007 du Parlement européen et du Conseil, le règlement (CE) n° 2007/2004 du Conseil et la décision 2005/267/CE du Conseil (JO L 251 du 16.9.2016, p. 1).

plan opérationnel relatif aux vérifications aux frontières, à la surveillance des frontières et au retour. D'autres agences de l'Union concernées, en particulier le Bureau européen d'appui en matière d'asile et Europol, peuvent également déployer, dans le cadre des équipes d'appui à la gestion des flux migratoires, des experts qui n'appartiennent pas au personnel de ces agences de l'Union. Le déploiement d'équipes du corps européen de garde-frontières et de garde-côtes, d'équipes d'agents impliqués dans les tâches liées aux retours et d'équipes d'appui à la gestion des flux migratoires a pour objectif de fournir des renforts techniques et opérationnels aux États membres demandeurs, en particulier à ceux confrontés à des défis migratoires disproportionnés. Pour accomplir les tâches qui leur sont confiées, ces différentes équipes ont besoin d'avoir accès au SIS grâce à une interface technique de l'Agence européenne de garde-frontières et de garde-côtes qui permette de se connecter au SIS central. Lorsqu'il ressort d'une consultation du SIS par l'équipe ou par les équipes d'agents qu'il existe un signalement introduit par un État membre, le membre de l'équipe ou l'agent ne peut exécuter la conduite à tenir requise que si l'État membre hôte l'y autorise. Il devrait dès lors informer l'État membre concerné pour lui permettre de donner suite à l'affaire.

(37) Conformément au règlement (UE) 2016/1624, l'Agence européenne de garde-frontières et de garde-côtes prépare des analyses des risques. Ces analyses portent sur tous les aspects pertinents pour la gestion européenne intégrée des frontières, notamment les menaces susceptibles d'affecter le fonctionnement ou la sécurité des frontières extérieures. Les signalements introduits dans le SIS conformément au présent règlement, en particulier les signalements aux fins de refus d'entrée et de séjour, sont des informations pertinentes pour évaluer les menaces éventuelles susceptibles d'affecter les frontières extérieures; l'Agence européenne de garde-frontières et de garde-côtes devrait donc pouvoir en disposer en vue de la préparation desdites analyses des risques. Pour accomplir les missions qui lui sont confiées en matière d'analyse des risques, il convient que l'Agence européenne de garde-frontières et de garde-côtes ait accès au SIS. En outre, conformément à la proposition de règlement du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), présentée par la Commission[55], l'unité centrale ETIAS de l'Agence européenne de garde-frontières et de garde-côtes effectuera des vérifications dans le SIS via l'ETIAS pour réaliser l'évaluation des demandes d'autorisation de voyage, qui requiert notamment de vérifier si le ressortissant de pays tiers qui demande une autorisation de voyage fait l'objet d'un signalement dans le SIS. À cet effet, l'unité centrale ETIAS au sein de l'Agence européenne de garde-frontières et de garde-côtes devrait avoir accès au SIS dans la mesure nécessaire à l'accomplissement de sa mission, c'est-à-dire à toutes les catégories de signalements de ressortissants de pays tiers qui font l'objet d'un signalement aux fins de refus d'entrée et de séjour ou d'une mesure restrictive visant à les empêcher d'entrer dans les États membres ou de transiter par eux.

(38) En raison de leur nature technique, de leur niveau de précision et de la nécessité de les actualiser à intervalles réguliers, certains aspects du SIS ne peuvent être couverts de manière exhaustive par les dispositions du présent règlement. Il s'agit, par exemple, des règles techniques concernant l'introduction, l'actualisation, la suppression et la consultation des données, de la qualité des données et des règles de consultation liées aux identifiants biométriques, des règles de compatibilité et de priorité entre les signalements, de l'apposition d'indicateurs de validité, de la mise en relation des

---

55 COM(2016) 731 final.

signalements, de la fixation de la date d'expiration des signalements dans les limites du délai maximal, et de l'échange d'informations supplémentaires. Les compétences d'exécution relatives à ces aspects devraient par conséquent être conférées à la Commission. Les règles techniques concernant les consultations de signalements devraient tenir compte du bon fonctionnement des applications nationales.

(39) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011[56]. La procédure d'adoption des mesures d'application à arrêter en vertu du présent règlement et du règlement (UE) 2018/xxx (sur la coopération policière et judiciaire) devrait être identique.

(40) Pour assurer la transparence, l'agence eu-LISA devrait présenter tous les deux ans un rapport sur le fonctionnement technique du SIS central et de l'infrastructure de communication, y compris la sécurité offerte, et sur les échanges d'informations supplémentaires. La Commission devrait procéder à une évaluation globale tous les quatre ans.

(41) Étant donné que les objectifs du présent règlement, à savoir l'établissement d'un système d'information commun et la fixation de règles applicables à ce dernier ainsi que l'échange d'informations supplémentaires, ne peuvent pas, de par leur nature même, être réalisés de manière suffisante par les États membres et peuvent donc être mieux réalisés au niveau de l'Union, l'Union peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(42) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus, notamment, par la Charte des droits fondamentaux de l'Union européenne. En particulier, il cherche à assurer un environnement sûr à toutes les personnes résidant sur le territoire de l'Union européenne et une protection des migrants en situation irrégulière contre l'exploitation et la traite des êtres humains, en permettant leur identification tout en respectant pleinement la protection des données à caractère personnel.

(43) Conformément aux articles 1er et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application. Le présent règlement développant l'acquis de Schengen, le Danemark décide, conformément à l'article 4 dudit protocole, dans un délai de six mois à partir de la décision du Conseil sur le présent règlement, s'il le transpose dans son droit interne.

(44) Le présent règlement constitue un développement des dispositions de l'acquis de Schengen auxquelles le Royaume-Uni ne participe pas, conformément à la décision 2000/365/CE du Conseil[57]; le Royaume-Uni ne participe donc pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application.

---

56 Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

57 JO L 131 du 1.6.2000, p. 43.

(45) Le présent règlement constitue un développement des dispositions de l'acquis de Schengen auxquelles l'Irlande ne participe pas, conformément à la décision 2002/192/CE du Conseil[58]; l'Irlande ne participe donc pas à l'adoption du présent règlement et n'est pas liée par celui-ci ni soumise à son application.

(46) En ce qui concerne l'Islande et la Norvège, le présent règlement constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[59] qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE du Conseil[60] relative à certaines modalités d'application de cet accord.

(47) En ce qui concerne la Suisse, le présent règlement constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord signé entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen qui relèvent des domaines visés à l'article 1er, point G, de la décision 1999/437/CE, lu en liaison avec l'article 4, paragraphe 1, de la décision 2004/849/CE du Conseil[61] et l'article 4, paragraphe 1, de la décision 2004/860/CE du Conseil[62].

(48) En ce qui concerne le Liechtenstein, le présent règlement constitue un développement des dispositions de l'acquis de Schengen au sens du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen[63] qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE, lu en liaison avec l'article 3 de la décision 2011/349/UE du Conseil[64] et l'article 3 de la décision 2011/350/UE du Conseil[65].

---

58 JO L 64 du 7.3.2002, p. 20.

59 JO L 176 du 10.7.1999, p. 36.

60 JO L 176 du 10.7.1999, p. 31.

61 Décision 2004/849/CE du Conseil du 25 octobre 2004 relative à la signature, au nom de l'Union européenne, et à l'application provisoire de certaines dispositions de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 368 du 15.12.2004, p. 26).

62 Décision 2004/860/CE du Conseil du 25 octobre 2004 relative à la signature, au nom de la Communauté européenne, et à l'application provisoire de certaines dispositions de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 370 du 17.12.2004, p. 78).

63 JO L 160 du 18.6.2011, p. 21.

64 Décision 2011/349/UE du Conseil du 7 mars 2011 relative à la conclusion, au nom de l'Union européenne, du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, notamment en ce qui concerne la coopération judiciaire en matière pénale et la coopération policière (JO L 160 du 18.6.2011, p. 1).

65 Décision 2011/350/UE du Conseil du 7 mars 2011 relative à la conclusion, au nom de l'Union européenne, du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord

(49) En ce qui concerne la Bulgarie et la Roumanie, le présent règlement constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte, au sens de l'article 4, paragraphe 2, de l'acte d'adhésion de 2005, et il doit être lu en combinaison avec la décision 2010/365/UE du Conseil sur l'application à la République de Bulgarie et à la Roumanie des dispositions de l'acquis de Schengen relatives au système d'information Schengen[66].

(50) En ce qui concerne Chypre et la Croatie, le présent règlement constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte, au sens, respectivement, de l'article 3, paragraphe 2, de l'acte d'adhésion de 2003 et de l'article 4, paragraphe 2, de l'acte d'adhésion de 2012.

(51) Le coût estimé de la mise à niveau des systèmes nationaux du SIS et de la mise en œuvre des nouvelles fonctionnalités envisagées dans le présent règlement est inférieur au solde restant dans la ligne budgétaire destinée aux frontières intelligentes dans le règlement (UE) n° 515/2014 du Parlement européen et du Conseil[67]. En conséquence, le présent règlement devrait réaffecter ce montant, attribué au développement de systèmes informatiques permettant la gestion des flux migratoires aux frontières extérieures, conformément à l'article 5, paragraphe 5, point b), du règlement (UE) n° 515/2014.

(52) Le règlement (CE) n° 1987/2006 devrait dès lors être abrogé.

(53) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, et a rendu son avis le […],

---

entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen en ce qui concerne la suppression des contrôles aux frontières intérieures et la circulation des personnes (JO L 160 du 18.6.2011, p. 19).

66 JO L 166 du 1.7.2010, p. 17.

67 Règlement (UE) n° 515/2014 du Parlement européen et du Conseil du 16 avril 2014 portant création, dans le cadre du Fonds pour la sécurité intérieure, de l'instrument de soutien financier dans le domaine des frontières extérieures et des visas (JO L 150 du 20.5.2014, p. 143).

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

# CHAPITRE I

## DISPOSITIONS GÉNÉRALES

*Article premier*
*Objectif général du SIS*

L'objet du SIS est d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, ainsi que d'appliquer les dispositions de la troisième partie, titre V, chapitre 2, du traité sur le fonctionnement de l'Union européenne relatives à la libre circulation des personnes sur les territoires des États membres, à l'aide des informations transmises par ce système.

*Article 2*
*Champ d'application*

1. Le présent règlement établit les conditions et les procédures relatives à l'introduction et au traitement dans le SIS des signalements de ressortissants de pays tiers, ainsi qu'à l'échange d'informations supplémentaires et de données complémentaires aux fins de refus d'entrée et de séjour sur le territoire des États membres.

2. Le présent règlement contient également des dispositions concernant l'architecture technique du SIS et les responsabilités incombant aux États membres et à l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, des règles générales sur le traitement des données, ainsi que des dispositions sur les droits des personnes concernées et sur la responsabilité.

*Article 3*
*Définitions*

1. Aux fins du présent règlement, on entend par:

   (a) «signalement», un ensemble de données, y compris les identifiants biométriques mentionnés à l'article 22, introduites dans le SIS pour permettre aux autorités compétentes d'identifier une personne en vue de tenir une conduite particulière à son égard;

   (b) «informations supplémentaires», les informations ne faisant pas partie des données d'un signalement stockées dans le SIS, mais en rapport avec des signalements introduits dans le SIS, qui doivent être échangées:

      (1) afin de permettre aux États membres de se consulter ou de s'informer mutuellement lors de l'introduction d'un signalement;

      (2) à la suite d'une réponse positive afin que la conduite à tenir demandée puisse être exécutée;

      (3) en cas d'impossibilité d'exécuter la conduite à tenir demandée;

      (4) en ce qui concerne la qualité des données du SIS;

      (5) en ce qui concerne la compatibilité et la priorité entre les signalements;

(6) en ce qui concerne l'exercice du droit d'accès;

(c) «données complémentaires», les données stockées dans le SIS et en rapport avec des signalements introduits dans le SIS, qui doivent être immédiatement accessibles aux autorités compétentes lorsqu'une personne au sujet de laquelle des données ont été introduites dans le SIS est localisée à la suite de consultations effectuées dans ce système;

(d) «ressortissant de pays tiers», toute personne qui n'est pas citoyen de l'Union au sens de l'article 20 du TFUE, à l'exception des personnes qui, en vertu d'accords conclus entre l'Union, ou l'Union et ses États membres, d'une part, et des pays tiers, d'autre part, jouissent de droits en matière de libre circulation équivalents à ceux des citoyens de l'Union;

(e) «données à caractère personnel», toute information concernant une personne physique identifiée ou identifiable («personne concernée»);

(f) «personne physique identifiable», une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

(g) «traitement de données à caractère personnel», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement dans un journal, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

(h) une «réponse positive» dans le SIS signifie que:

(1) une consultation est effectuée par un utilisateur,

(2) il ressort de la consultation qu'il existe un signalement introduit par un autre État membre dans le SIS,

(3) les données relatives au signalement introduit dans le SIS correspondent aux données de la consultation, et

(4) une conduite à tenir est demandée en conséquence de la réponse positive;

(i) «État membre signalant», l'État membre qui introduit le signalement dans le SIS;

(j) «État membre d'exécution», l'État membre qui exécute la conduite à tenir à la suite d'une réponse positive;

(k) «utilisateurs finaux», les autorités compétentes qui consultent directement le CS-SIS, le N.SIS ou une copie technique de ceux-ci;

(l) «retour» le retour défini à l'article 3, point 3, de la directive 2008/115/CE;

(m) «interdiction d'entrée» l'interdiction d'entrée définie à l'article 3, point 6, de la directive 2008/115/CE;

(n) «données dactylographiques», les données relatives aux empreintes digitales et empreintes palmaires qui, en raison de leur caractère unique et des points de

référence qu'elles contiennent, permettent de réaliser des comparaisons précises et concluantes en ce qui concerne l'identité d'une personne;

(o) «infractions graves», les infractions énumérées à l'article 2, paragraphes 1 et 2, de la décision-cadre 2002/584/JAI du 13 juin 2002[68];

(p) «infractions terroristes», les infractions prévues par le droit national visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI du 13 juin 2002[69].

*Article 4*
*Architecture technique et mode de fonctionnement du SIS*

1. Le SIS se compose:

(a) d'un système central (le «SIS central») comprenant:

– une fonction de support technique (le «CS-CIS») contenant la base de données du SIS;

– une interface nationale uniforme (le «NI-SIS»);

(b) d'une section nationale (le «N.SIS») dans chaque État membre, constituée des systèmes de données nationaux reliés au SIS central. Un N.SIS contient un fichier de données (une «copie nationale») comprenant une copie complète ou partielle de la base de données du SIS ainsi qu'un N.SIS de secours. Le N.SIS et sa version de secours peuvent être utilisés simultanément en vue d'assurer la disponibilité continue pour les utilisateurs finaux;

(c) d'une infrastructure de communication entre le CS-SIS et le NI-SIS (l'«infrastructure de communication»), fournissant un réseau virtuel crypté consacré aux données du SIS et à l'échange de données entre les bureaux SIRENE visés à l'article 7, paragraphe 2.

2. Les données du SIS sont introduites, mises à jour, supprimées et consultées par le biais des différents N.SIS. Une copie nationale partielle ou complète est disponible pour effectuer des consultations automatisées sur le territoire de chacun des États membres utilisant une telle copie. La copie nationale partielle contient au moins les données mentionnées à l'article 20, paragraphe 2, points a) à v), du présent règlement. Il n'est pas possible de consulter les fichiers de données des N.SIS des autres États membres.

3. Le CS-SIS assure des fonctions techniques de contrôle et de gestion, et dispose d'un CS-SIS de secours capable d'assurer l'ensemble des fonctionnalités du CS-SIS principal en cas de défaillance de celui-ci. Le CS-SIS et sa version de secours sont installés sur les deux sites techniques de l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, créée par le règlement (UE) n° 1077/2011[70] (l'«agence eu-LISA»). Le CS-SIS ou sa version de secours peuvent contenir une copie supplémentaire de la base de données du SIS et être utilisés simultanément en

---

68 Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

69 Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

70 Instituée par le règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (JO L 286 du 1.11.2011, p. 1).

fonctionnement actif, à condition que chacun d'eux soit capable de traiter toutes les transactions liées aux signalements introduits dans le SIS.

4. Le CS-SIS assure les services nécessaires à l'introduction et au traitement des données du SIS, y compris les consultations dans la base de données du SIS. Le CS-SIS assure:

   (a) la mise à jour en ligne de la copie nationale;

   (b) la synchronisation et la cohérence entre la copie nationale et la base de données du SIS;

   (c) les opérations d'initialisation et de restauration de la copie nationale;

   (d) la disponibilité continue.

*Article 5*
*Coûts*

1. Les coûts d'exploitation, de maintenance et de développement ultérieur du SIS central et de l'infrastructure de communication sont à la charge du budget général de l'Union européenne.

2. Ces coûts couvrent les travaux effectués en ce qui concerne le CS-SIS afin d'assurer la fourniture des services visés à l'article 4, paragraphe 4.

3. Les coûts de mise en place, d'exploitation, de maintenance et de développement ultérieur de chaque N.SIS sont à la charge de l'État membre concerné.

# CHAPITRE II

## RESPONSABILITÉS INCOMBANT AUX ÉTATS MEMBRES

*Article 6*
*Systèmes nationaux*

Chaque État membre est chargé de mettre en place, d'exploiter et de continuer à développer son N.SIS, ainsi que d'en assurer la maintenance, et de le connecter au NI-SIS.

Chaque État membre est chargé d'assurer le fonctionnement continu du N.SIS, sa connexion au NI-SIS et la disponibilité continue des données du SIS pour les utilisateurs finaux.

*Article 7*
*Office N.SIS et bureau SIRENE*

1. Chaque État membre désigne une autorité (l'«office N.SIS») qui assume la responsabilité centrale du N.SIS.

   Cette autorité est responsable du bon fonctionnement et de la sécurité du N.SIS, fait en sorte que les autorités compétentes aient accès au SIS et prend les mesures nécessaires pour assurer le respect des dispositions du présent règlement. Elle est chargée de veiller à ce que toutes les fonctionnalités du SIS soient dûment mises à la disposition des utilisateurs finaux.

   Chaque État membre transmet ses signalements par l'intermédiaire de son office N.SIS.

2. Chaque État membre désigne l'autorité chargée d'assurer l'échange et la disponibilité de toutes les informations supplémentaires (le «bureau SIRENE»), conformément aux dispositions du manuel SIRENE, tel que visé à l'article 8.

Ces bureaux coordonnent également la vérification de la qualité des informations introduites dans le SIS. À ces fins, ils ont accès aux données traitées dans le SIS.

3. Les États membres communiquent à l'agence eu-LISA les coordonnées de leur office N.SIS et de leur bureau SIRENE. L'agence eu-LISA publie la liste de ces coordonnées ainsi que celle visée à l'article 36, paragraphe 8.

*Article 8*
*Échange d'informations supplémentaires*

1. Les informations supplémentaires sont échangées conformément aux dispositions du manuel SIRENE, au moyen de l'infrastructure de communication. Les États membres fournissent les moyens techniques et humains nécessaires pour assurer la disponibilité permanente et l'échange d'informations supplémentaires. Au cas où l'infrastructure de communication ne serait pas accessible, les États membres peuvent utiliser d'autres moyens techniques correctement sécurisés pour échanger des informations supplémentaires.

2. Les informations supplémentaires sont utilisées exclusivement aux fins auxquelles elles ont été transmises, conformément à l'article 43, sauf accord préalable de l'État membre signalant.

3. Les bureaux SIRENE s'acquittent de leur tâche de manière rapide et efficace, notamment en répondant aux demandes dans les meilleurs délais, au plus tard 12 heures après leur réception.

4. Les modalités relatives à l'échange d'informations supplémentaires sont adoptées au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 55, paragraphe 2, sous la forme du «manuel SIRENE».

*Article 9*
*Conformité technique et fonctionnelle*

1. Pour permettre une transmission rapide et efficace des données, chaque État membre applique, lors de la création de son N.SIS, les normes communes, les protocoles et les procédures techniques établis afin de permettre la compatibilité de son N.SIS avec le CS-SIS. Ces normes communes, protocoles et procédures techniques sont établis et élaborés au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

2. Les États membres veillent, au moyen des services fournis par le CS-SIS et des mises à jour automatiques visées à l'article 4, paragraphe 4, à ce que les données stockées dans la copie nationale soient identiques à celles de la base de données du SIS et compatibles avec elles, et à ce qu'une consultation de cette copie produise un résultat équivalent à celui d'une consultation dans la base de données du SIS. Les utilisateurs finaux reçoivent les données dont ils ont besoin pour s'acquitter de leurs tâches, en particulier, toutes les données nécessaires pour identifier la personne concernée et exécuter la conduite à tenir demandée.

*Article 10*
*Sécurité - États membres*

1. Chaque État membre adopte, pour son N.SIS, les mesures, dont un plan de sécurité, un plan de continuité des opérations et un plan de rétablissement après sinistre, propres à:

   (a) assurer la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques;

   (b) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle de l'accès aux installations);

   (c) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);

   (d) empêcher l'introduction non autorisée de données ainsi que tout examen, toute modification ou tout effacement non autorisés de données à caractère personnel stockées (contrôle du stockage);

   (e) empêcher que les systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées au moyen de matériel de transmission de données (contrôle des utilisateurs);

   (f) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données pour lesquelles elles ont une autorisation d'accès et uniquement grâce à des identités d'utilisateur individuelles et uniques ainsi qu'à des modes d'accès confidentiels (contrôle de l'accès aux données);

   (g) garantir que toutes les autorités ayant un droit d'accès au SIS ou aux installations de traitement de données créent des profils décrivant les tâches et responsabilités qui incombent aux personnes habilitées en matière d'accès, d'introduction, de mise à jour, de suppression et de consultation des données et mettent sans tarder et à leur demande ces profils à la disposition des autorités de contrôle nationales visées à l'article 50, paragraphe 1 (profils des membres du personnel);

   (h) garantir qu'il puisse être vérifié et constaté à quels organismes des données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données (contrôle de la transmission);

   (i) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, à quel moment, par qui et à quelle fin (contrôle de l'introduction);

   (j) empêcher, en particulier par des techniques de cryptage adaptées, que, lors de la transmission de données à caractère personnel ou du transport de support de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport);

   (k) contrôler l'efficacité des mesures de sécurité prévues au présent paragraphe et prendre les mesures organisationnelles nécessaires en matière de contrôle interne (autosurveillance).

2. Les États membres prennent des mesures équivalentes à celles visées au paragraphe 1 pour assurer la sécurité du traitement et des échanges d'informations supplémentaires, y compris la sécurisation des locaux du bureau SIRENE.

3. Les États membres prennent des mesures équivalentes à celles visées au paragraphe 1 pour assurer la sécurité du traitement des données du SIS effectué par les autorités mentionnées à l'article 29.

*Article 11*
*Confidentialité - États membres*

Chaque État membre applique à l'égard de toutes les personnes et de tous les organismes appelés à travailler avec des données du SIS et des informations supplémentaires ses règles relatives au secret professionnel ou leur impose des obligations de confidentialité équivalentes, conformément à sa législation nationale. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après que ces organismes ont cessé leur activité.

*Article 12*
*Tenue de journaux au niveau national*

1. Les États membres veillent à ce que tout accès à des données à caractère personnel et tout échange de ces données avec le CS-SIS soient enregistrés dans le N.SIS afin de pouvoir contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS, ainsi que l'intégrité et la sécurité des données.

2. Les journaux d'enregistrement indiquent, en particulier, l'historique du signalement, la date et l'heure de l'opération de traitement des données, le type de données utilisées pour effectuer une consultation, le type de données transmises et les noms de l'autorité compétente et de la personne chargée du traitement des données.

3. Si la consultation est effectuée à partir de données dactylographiques ou d'une image faciale conformément à l'article 22, les journaux indiquent, notamment, le type de données utilisées pour la consultation, le type de données transmises et les noms de l'autorité compétente et de la personne chargée du traitement des données.

4. Les journaux ne peuvent être utilisés que pour la finalité visée au paragraphe 1 et sont supprimés au plus tôt un an et au plus tard trois ans après leur création.

5. Les journaux peuvent être conservés plus longtemps s'ils sont nécessaires à une procédure de contrôle déjà engagée.

6. Les autorités nationales compétentes chargées de contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS, ainsi que l'intégrité et la sécurité des données, ont accès, dans les limites de leurs compétences et sur demande, à ces journaux afin de pouvoir s'acquitter de leurs tâches.

*Article 13*
*Autocontrôle*

Les États membres veillent à ce que chaque autorité autorisée à avoir accès aux données du SIS prenne les mesures nécessaires pour se conformer au présent règlement et coopère, si nécessaire, avec l'autorité de contrôle nationale.

*Article 14*
*Formation du personnel*

Avant d'être autorisé à traiter des données stockées dans le SIS, puis à intervalles réguliers après avoir obtenu l'accès à ces données, le personnel des autorités qui a un droit d'accès au SIS reçoit une formation appropriée sur les règles en matière de sécurité et de protection des données et sur les procédures relatives au traitement des données fixées dans le manuel SIRENE. Ce personnel est informé des infractions et sanctions pénales éventuelles en la matière.

# CHAPITRE III

## RESPONSABILITÉS DE L'AGENCE EU-LISA

*Article 15*
*Gestion opérationnelle*

1. L'agence eu-LISA est chargée de la gestion opérationnelle du SIS central. Elle veille, en coopération avec les États membres, à ce que le SIS central bénéficie en permanence de la meilleure technologie disponible, sur la base d'une analyse coût-avantages.

2. Il incombe également à l'agence eu-LISA d'assurer les tâches suivantes en ce qui concerne l'infrastructure de communication:

   (a) supervision;

   (b) sécurité;

   (c) coordination des relations entre les États membres et le fournisseur.

3. La Commission est chargée de toutes les autres tâches liées à l'infrastructure de communication, en particulier:

   (a) les tâches relatives à l'exécution du budget;

   (b) les acquisitions et renouvellements;

   (c) les questions contractuelles.

4. L'agence eu-LISA est également chargée des tâches suivantes en ce qui concerne les bureaux SIRENE et la communication entre ces bureaux:

   (a) la coordination et la gestion des tests;

   (b) la gestion et la mise à jour des spécifications techniques relatives à l'échange d'informations supplémentaires entre les bureaux SIRENE et l'infrastructure de communication, ainsi que la gestion des effets des modifications techniques lorsqu'elles ont une incidence sur le SIS et sur les échanges d'informations supplémentaires entre les bureaux SIRENE.

5. L'agence eu-LISA élabore et gère un dispositif et des procédures de contrôle de qualité des données du CS-SIS et présente des rapports réguliers aux États membres. Elle présente à la Commission un rapport régulier indiquant les problèmes rencontrés et les États membres concernés. Le dispositif, les procédures et l'interprétation relative à la qualité conforme des données sont établis et élaborés au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

6. La gestion opérationnelle du SIS central comprend toutes les tâches nécessaires pour que le SIS central puisse fonctionner 24 heures sur 24, 7 jours sur 7 conformément au présent règlement, en particulier les travaux de maintenance et les développements techniques indispensables au bon fonctionnement du système. Elles incluent également les tests destinés à vérifier que le SIS central et les systèmes nationaux fonctionnent conformément aux exigences techniques et fonctionnelles prévues à l'article 9 du présent règlement.

*Article 16*
*Sécurité*

1. L'agence eu-LISA adopte, pour le SIS central et l'infrastructure de communication, les mesures, dont un plan de sécurité, un plan de continuité des opérations et un plan de rétablissement après sinistre, propres à:

(a) assurer la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques;

(b) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle de l'accès aux installations);

(c) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);

(d) empêcher l'introduction non autorisée de données ainsi que tout examen, toute modification ou tout effacement non autorisés de données à caractère personnel stockées (contrôle du stockage);

(e) empêcher que les systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées au moyen de matériel de transmission de données (contrôle des utilisateurs);

(f) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données pour lesquelles elles ont une autorisation d'accès et uniquement grâce à des identités d'utilisateur individuelles et uniques ainsi qu'à des modes d'accès confidentiels (contrôle de l'accès aux données);

(g) assurer la création de profils décrivant les tâches et responsabilités qui incombent aux personnes habilitées en matière d'accès aux données ou aux installations de traitement de données, et la mise de ces profils à la disposition du Contrôleur européen de la protection des données visé à l'article 51, sans tarder et à la demande de celui-ci (profils des membres du personnel);

(h) garantir qu'il puisse être vérifié et constaté à quels organismes des données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données (contrôle de la transmission);

(i) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, à quel moment et par qui (contrôle de l'introduction);

(j) empêcher, en particulier par des techniques de cryptage adaptées, que, lors de la transmission de données à caractère personnel ou du transport de support de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport);

(k) contrôler l'efficacité des mesures de sécurité visées au présent paragraphe et prendre les mesures d'organisation en matière de contrôle interne qui sont nécessaires au respect du présent règlement (autosurveillance).

2. L'agence eu-LISA prend des mesures équivalentes à celles visées au paragraphe 1 pour assurer la sécurité du traitement et de l'échange d'informations supplémentaires par le biais de l'infrastructure de communication.

*Article 17*
*Confidentialité – Agence eu-LISA*

1. Sans préjudice de l'article 17 du statut des fonctionnaires et du régime applicable aux autres agents de l'Union européenne, l'agence eu-LISA applique des règles appropriées en matière de secret professionnel, ou impose des obligations de confidentialité équivalentes, qui s'appliquent à tous les membres de son personnel appelés à travailler avec des données du SIS et répondent à des normes comparables à celles prévues à l'article 11 du présent règlement. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après la fin de leurs activités.

2. L'agence eu-LISA prend des mesures équivalentes à celles visées au paragraphe 1 pour assurer la confidentialité de l'échange d'informations supplémentaires par le biais de l'infrastructure de communication.

*Article 18*
*Tenue de journaux au niveau central*

1. L'agence eu-LISA veille à ce que tous les accès aux données à caractère personnel et tous les échanges de telles données contenues dans le CS-SIS soient enregistrés aux fins mentionnées à l'article 12, paragraphe 1.

2. Les journaux indiquent, en particulier, l'historique des signalements, la date et l'heure de la transmission des données, le type de données utilisées pour effectuer des consultations, le type de données transmises et le nom de l'autorité compétente chargée du traitement des données.

3. Si la consultation est effectuée à partir de données dactylographiques ou d'une image faciale conformément aux articles 22 et 28, les journaux indiquent, notamment, le type de données utilisées pour la consultation, le type de données transmises et les noms de l'autorité compétente et de la personne chargée du traitement des données.

4. Les journaux ne peuvent être utilisés qu'aux fins mentionnées au paragraphe 1, et sont supprimés au plus tôt un an et au plus tard trois ans après leur création. Les journaux contenant l'historique des signalements sont effacés de un à trois ans après la suppression des signalements.

5. Les journaux peuvent être conservés plus longtemps s'ils sont nécessaires à une procédure de contrôle déjà engagée.

6. Les autorités compétentes chargées de contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du CS-SIS, ainsi que l'intégrité et la sécurité des données, ont accès, dans les limites de leurs compétences et à leur demande, à ces journaux afin de pouvoir s'acquitter de leurs tâches.

# CHAPITRE IV

# INFORMATION DU PUBLIC

*Article 19*
*Campagnes d'information sur le SIS*

La Commission, en coopération avec les autorités de contrôle nationales et le Contrôleur européen de la protection des données, organise régulièrement des campagnes visant à faire connaître au public les objectifs du SIS, les données stockées, les autorités disposant d'un droit d'accès au SIS et les droits des personnes concernées. Les États membres, en coopération avec leurs autorités de contrôle nationales, élaborent et mettent en œuvre les politiques nécessaires pour assurer l'information générale de leurs citoyens sur le SIS.

# CHAPITRE V

## SIGNALEMENTS DE RESSORTISSANTS DE PAYS TIERS AUX FINS DE REFUS D'ENTRÉE ET DE SÉJOUR

*Article 20*
*Catégories de données*

1. Sans préjudice des dispositions de l'article 8, paragraphe 1, ou des dispositions du présent règlement prévoyant le stockage de données complémentaires, le SIS comporte exclusivement les catégories de données qui sont fournies par chacun des États membres et qui sont nécessaires aux fins prévues à l'article 24.

2. Les renseignements concernant les personnes signalées comprennent uniquement les données suivantes:

   (a) le(s) nom(s);

   (b) le(s) prénom(s);

   (c) le(s) nom(s) à la naissance;

   (d) les noms utilisés antérieurement et les pseudonymes;

   (e) les signes physiques particuliers, objectifs et inaltérables;

   (f) le lieu de naissance;

   (g) la date de naissance;

   (h) le sexe;

   (i) la ou les nationalités;

   (j) l'indication que la personne concernée est armée, violente, en fuite ou impliquée dans une activité mentionnée aux articles 1er, 2, 3 ou 4 de la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme;

   (k) le motif du signalement;

   (l) l'autorité signalante;

(m) une référence à la décision qui est à l'origine du signalement;

(n) la conduite à tenir;

(o) le(s) lien(s) vers d'autres signalements introduits dans le SIS conformément à l'article 38;

(p) l'indication que la personne concernée est un membre de la famille d'un citoyen de l'Union ou une autre personne jouissant de droits en matière de libre circulation tels que visés à l'article 25;

(q) l'indication que la décision de refus d'entrée est fondée sur:

– une condamnation antérieure telle que visée à l'article 24, paragraphe 2, point a);

– une menace grave pour la sécurité telle que visée à l'article 24, paragraphe 2, point b);

– une interdiction d'entrée telle que visée à l'article 24, paragraphe 3; ou

– une mesure restrictive telle que visée à l'article 27;

(r) le type d'infraction (pour les signalements introduits en vertu de l'article 24, paragraphe 2, du présent règlement);

(s) la catégorie du document d'identification de la personne;

(t) le pays de délivrance du document d'identification de la personne;

(u) le(s) numéro(s) du document d'identification de la personne;

(v) la date de délivrance du document d'identification de la personne;

(w) les photographies et images faciales;

(x) les données dactylographiques;

(y) une copie en couleurs du document d'identification.

3. Les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées au paragraphe 2 sont établies et élaborées au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

4. Les règles techniques nécessaires pour la consultation des données visées au paragraphe 2 sont établies et élaborées conformément à la procédure d'examen visée à l'article 55, paragraphe 2. Ces règles techniques sont similaires pour les consultations dans le CS-SIS, dans les copies nationales et dans les copies techniques visées à l'article 36, et elles sont fondées sur des normes communes établies et élaborées au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

*Article 21*
*Proportionnalité*

1. Avant d'introduire un signalement et de prolonger la durée de validité de ce dernier, l'État membre vérifie si le dossier est suffisamment approprié, pertinent et important pour justifier l'introduction du signalement dans le SIS.

2. Lors de l'application de l'article 24, paragraphe 2, les États membres introduisent, en toutes circonstances, le signalement correspondant relatif à un ressortissant de pays

tiers si l'infraction concernée relève des articles 1er à 4 de la décision-cadre 2002/475/JAI du Conseil relative à la lutte contre le terrorisme[71].

*Article 22*

*Règles spécifiques pour l'introduction de photographies, d'images faciales et de données dactylographiques*

1. Les données mentionnées à l'article 20, paragraphe 2, points w) et x), ne sont introduites dans le SIS qu'après avoir été soumises à un contrôle de qualité visant à garantir le respect de normes minimales en matière de qualité des données.

2. Des normes de qualité sont définies pour le stockage des données visées au paragraphe 1. Leur contenu est déterminé et actualisé au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

*Article 23*

*Exigence à remplir pour l'introduction d'un signalement*

1. Un signalement ne peut être introduit sans les données mentionnées à l'article 20, paragraphe 2, points a), g), k), m), n) et q). Lorsqu'un signalement se fonde sur une décision prise en vertu de l'article 24, paragraphe 2, les données mentionnées à l'article 20, paragraphe 2, point r), sont également introduites.

2. Lorsqu'elles sont disponibles, toutes les autres données énumérées à l'article 20, paragraphe 2, sont aussi introduites.

*Article 24*

*Conditions auxquelles sont soumis les signalements introduits aux fins de refus d'entrée et de séjour*

1. Les données relatives aux ressortissants de pays tiers faisant l'objet d'un signalement aux fins de refus d'entrée et de séjour sont introduites dans le SIS sur le fondement d'un signalement national résultant d'une décision prise par les autorités administratives ou judiciaires compétentes dans le respect des règles de procédure prévues par la législation nationale, sur la base d'une évaluation individuelle. Les recours contre ces décisions sont formés conformément au droit national.

2. Un signalement est introduit lorsque la décision visée au paragraphe 1 est fondée sur la menace, pour l'ordre public ou la sécurité publique ou pour la sécurité nationale, que peut constituer la présence d'un ressortissant de pays tiers sur le territoire d'un État membre. Tel peut être notamment le cas:

   (a) d'un ressortissant de pays tiers qui a été condamné dans un État membre pour une infraction passible d'une peine privative de liberté d'au moins un an;

   (b) d'un ressortissant de pays tiers à l'égard duquel il existe des raisons sérieuses de croire qu'il a commis une infraction grave, ou à l'égard duquel il existe des indices manifestes d'une intention de commettre une telle infraction sur le territoire d'un État membre.

---

[71] Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (JO L 164 du 22.6.2002, p. 3).

3. Un signalement est introduit lorsque la décision visée au paragraphe 1 est une interdiction d'entrée prononcée selon des procédures respectant la directive 2008/115/CE. L'État membre signalant veille à ce que le signalement prenne effet dans le SIS au moment du retour du ressortissant de pays tiers concerné. La confirmation du retour est communiquée à l'État membre signalant conformément à l'article 6 du règlement (UE) 2018/xxx [règlement sur le retour].

*Article 25*
*Conditions auxquelles sont soumis les signalements de ressortissants de pays tiers jouissant du droit de libre circulation dans l'Union*

1. Un signalement concernant un ressortissant de pays tiers qui jouit du droit de libre circulation dans l'Union au sens de la directive 2004/38/CE du Parlement européen et du Conseil[72] est introduit conformément aux mesures adoptées pour transposer ladite directive.

2. En cas de réponse positive concernant un signalement, introduit en vertu de l'article 24, relatif à un ressortissant de pays tiers qui jouit du droit de libre circulation dans l'Union, l'État membre d'exécution consulte immédiatement l'État membre signalant, par voie d'échange d'informations supplémentaires, afin de décider sans délai de la conduite à tenir.

*Article 26*
*Procédure de consultation*

1. Lorsqu'un État membre envisage d'accorder un titre de séjour ou une autre autorisation conférant un droit de séjour à un ressortissant de pays tiers faisant l'objet d'un signalement aux fins de refus d'entrée et de séjour introduit par un autre État membre, il consulte au préalable l'État membre signalant, par voie d'échange d'informations supplémentaires, et tient compte des intérêts de cet État membre. L'État membre signalant fournit une réponse définitive dans un délai de sept jours. Lorsque l'État membre envisageant d'accorder un titre de séjour ou une autre autorisation conférant un droit de séjour décide d'accorder ce titre ou cette autorisation, le signalement aux fins de refus d'entrée et de séjour est supprimé.

2. Lorsqu'un État membre envisage d'introduire un signalement aux fins de refus d'entrée et de séjour concernant un ressortissant de pays tiers qui est titulaire d'un titre de séjour valable ou d'une autre autorisation conférant un droit de séjour délivré par un autre État membre, il consulte au préalable l'État membre qui a délivré le titre ou l'autorisation, par voie d'échange d'informations supplémentaires, et tient compte des intérêts de cet État membre. L'État membre qui a délivré le titre ou l'autorisation fournit une réponse définitive dans un délai de sept jours. Si l'État membre de délivrance décide de maintenir le titre ou l'autorisation, le signalement aux fins de refus d'entrée et de séjour n'est pas introduit.

3. En cas de réponse positive concernant un signalement aux fins de refus d'entrée et de séjour qui vise un ressortissant de pays tiers qui est titulaire d'un titre de séjour valable ou d'une autre autorisation conférant un droit de séjour, l'État membre d'exécution consulte immédiatement l'État membre qui a délivré le titre ou l'autorisation et l'État membre qui a introduit le signalement, respectivement, par voie d'échange d'informations supplémentaires, afin de décider sans délai si la

[72] JO L 158 du 30.4.2004, p. 77.

conduite à tenir peut être exécutée. S'il est décidé de maintenir le titre ou l'autorisation de séjour, le signalement est supprimé.

4. Les États membres fournissent annuellement à l'agence eu-LISA des statistiques sur les consultations menées conformément aux paragraphes 1 à 3.

*Article 27*

*Conditions auxquelles sont soumis les signalements de ressortissants de pays tiers qui font l'objet de mesures restrictives*

1. Les signalements relatifs à des ressortissants de pays tiers qui font l'objet d'une mesure restrictive destinée à empêcher qu'ils entrent sur le territoire des États membres ou qu'ils transitent par ce territoire, prise conformément à des actes juridiques adoptés par le Conseil, y compris les mesures mettant en œuvre une interdiction de voyage décrétée par le Conseil de sécurité des Nations unies, font, dans la mesure où il peut être satisfait aux exigences en matière de qualité des données, l'objet d'une introduction dans le SIS aux fins de refus d'entrée et de séjour.

2. L'État membre responsable de l'introduction, de la mise à jour et de la suppression de ces signalements au nom de tous les États membres est désigné lors de l'adoption de la mesure en question prise au titre de l'article 29 du traité sur l'Union européenne. La procédure de désignation de l'État membre responsable est établie et élaborée au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

# CHAPITRE VI

## CONSULTATION À L'AIDE DE DONNÉES BIOMÉTRIQUES

*Article 28*

*Règles spécifiques pour les vérifications ou les consultations à l'aide de photographies, d'images faciales et de données dactylographiques*

1. Les photographies, les images faciales et les données dactylographiques sont extraites du SIS pour vérifier l'identité d'une personne localisée à la suite d'une consultation alphanumérique effectuée dans le SIS.

2. Les données dactylographiques peuvent aussi être utilisées pour identifier une personne. Les données dactylographiques stockées dans le SIS sont utilisées à des fins d'identification si l'identité de la personne ne peut être établie par d'autres moyens.

3. Les données dactylographiques stockées dans le SIS en rapport avec des signalements introduits en vertu de l'article 24 peuvent également faire l'objet de consultations à l'aide de séries complètes ou incomplètes d'empreintes digitales ou d'empreintes palmaires découvertes sur les lieux d'infractions faisant l'objet d'une enquête, lorsqu'il peut être établi, avec un degré élevé de probabilité, qu'elles appartiennent à l'auteur de l'infraction, pour autant que les autorités compétentes ne puissent pas établir l'identité de la personne en recourant à toute autre base de données nationale, européenne ou internationale.

4. Dès que cela est techniquement possible tout en assurant un haut degré de fiabilité de l'identification, les photographies et les images faciales peuvent être utilisées pour identifier une personne. L'identification à l'aide de photographies ou d'images faciales n'est utilisée que dans le contexte des points de franchissement régulier des frontières équipés de systèmes en libre service et de systèmes de contrôle automatisé aux frontières.

# CHAPITRE VII

## DROIT D'ACCÈS ET CONSERVATION DES SIGNALEMENTS

*Article 29*
*Autorités disposant d'un droit d'accès aux signalements*

1. L'accès aux données introduites dans le SIS ainsi que le droit de les consulter, directement ou dans une copie, sont réservés aux autorités chargées de l'identification de ressortissants de pays tiers, aux fins:

   (a) du contrôle aux frontières, conformément au 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);

   (b) des vérifications de police et de douanes effectuées à l'intérieur de l'État membre concerné et de la coordination de celles-ci par les autorités désignées;

   (c) des autres actions répressives menées à des fins de prévention et de détection des infractions pénales ainsi que d'enquêtes en la matière avec l'État membre concerné;

   (d) de l'examen des conditions et de l'adoption des décisions relatives à l'entrée et au séjour des ressortissants de pays tiers sur le territoire des États membres, y compris en matière de titres de séjour et de visas de long séjour, ainsi qu'au retour des ressortissants de pays tiers;

   (e) de l'examen des demandes de visa et de l'adoption des décisions y relatives, notamment les décisions d'annulation, d'abrogation ou de prolongation des visas, conformément au règlement (CE) nº 810/2009 du Parlement européen et du Conseil[73].

2. Aux fins de l'article 24, paragraphes 2 et 3, et de l'article 27, le droit d'accès aux données introduites dans le SIS et le droit de les consulter directement peuvent également être exercés par les autorités judiciaires nationales, y compris celles qui sont compétentes pour engager des poursuites judiciaires dans le cadre de procédures pénales et des enquêtes judiciaires avant l'inculpation, dans l'exercice de leurs fonctions, conformément à la législation nationale, et par leurs autorités de coordination.

3. Le droit d'accès aux données concernant des documents relatifs à des personnes, introduites conformément à l'article 38, paragraphe 2, points j) et k), du règlement (UE) 2018/xxx [coopération policière et coopération judiciaire en matière pénale], et le droit de consulter ces données peuvent également être exercés par les

[73] Règlement (CE) nº 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (code des visas) (JO L 243 du 15.9.2009, p. 1).

autorités visées au paragraphe 1, point d). L'accès de ces autorités aux données est régi par le droit national de chaque État membre.

4. Les autorités visées au présent article sont incluses dans la liste mentionnée à l'article 36, paragraphe 8.

*Article 30*
*Accès d'Europol aux données du SIS*

1. L'Agence de l'Union européenne pour la coopération des services répressifs (Europol) a, dans les limites de son mandat, le droit d'accéder aux données introduites dans le SIS et de les consulter.

2. Lorsqu'il ressort d'une consultation du système par Europol qu'il existe un signalement dans le SIS, Europol en informe l'État membre signalant par les canaux définis dans le règlement (UE) 2016/794.

3. L'utilisation des informations obtenues lors d'une consultation du SIS est soumise à l'accord de l'État membre concerné. Si ledit État membre autorise l'utilisation de ces informations, leur traitement par Europol est régi par le règlement (UE) 2016/794. Europol ne peut communiquer ces informations à des pays ou organismes tiers qu'avec le consentement de l'État concerné.

4. Europol peut demander d'autres informations à l'État membre concerné, conformément aux dispositions du règlement (UE) 2016/794.

5. Europol doit:

   (a) sans préjudice des paragraphes 3, 4 et 6, s'abstenir de connecter les parties du SIS auxquelles il a accès à un système informatisé de collecte et de traitement des données exploité par Europol ou en son sein et de transférer les données qu'elles contiennent vers un tel système, ainsi que de télécharger ou de copier, de toute autre manière, une quelconque partie du SIS;

   (b) limiter l'accès aux données introduites dans le SIS au personnel expressément autorisé d'Europol;

   (c) adopter et appliquer les mesures prévues aux articles 10 et 11;

   (d) autoriser le Contrôleur européen de la protection des données à contrôler les activités qu'Europol mène dans le cadre de l'exercice de son droit d'accès aux données introduites dans le SIS et de son droit de consulter lesdites données.

6. Les données ne peuvent être copiées qu'à des fins techniques, pour autant que cette copie soit nécessaire au personnel dûment autorisé d'Europol pour effectuer une consultation directe. Les dispositions du présent règlement s'appliquent à ces copies. La copie technique est utilisée aux fins du stockage de données du SIS pendant la consultation de ces données. Les données sont supprimées dès qu'elles ont été consultées. De telles utilisations ne sont pas considérées comme des téléchargements ou copies illicites de données du SIS. Europol s'abstient de copier des données de signalements ou des données complémentaires transmises par les États membres, ou des données provenant du CS-SIS, vers d'autres systèmes d'Europol.

7. Les copies visées au paragraphe 6 alimentant des bases de données hors ligne ne peuvent être conservées que pour une durée inférieure à 48 heures. Cette durée peut être prolongée dans une situation d'urgence jusqu'à ce que cette situation d'urgence prenne fin. Europol signale toute prolongation de ce type au Contrôleur européen de la protection des données.

8. Europol peut recevoir et traiter des informations supplémentaires relatives aux signalements correspondants introduits dans le SIS, pour autant que les règles de traitement des données visées aux paragraphes 2 à 7 soient appliquées s'il y a lieu.

9. Aux fins de vérifier la licéité du traitement des données, d'assurer un autocontrôle ainsi que de garantir la sécurité et l'intégrité des données, Europol doit enregistrer dans des journaux tout accès au SIS et toute consultation de celui-ci. De tels journaux ne sont pas considérés comme des téléchargements ou copies illicites d'une quelconque partie du SIS.

*Article 31*

*Accès aux données du SIS par les équipes du corps européen de garde-frontières et de garde-côtes, les équipes d'agents impliqués dans les tâches liées aux retours et les membres des équipes d'appui à la gestion des flux migratoires*

1. Conformément à l'article 40, paragraphe 8, du règlement (UE) 2016/1624, les membres des équipes du corps européen de garde-frontières et de garde-côtes ou des équipes d'agents impliqués dans les tâches liées aux retours, ainsi que les membres des équipes d'appui à la gestion des flux migratoires ont le droit, dans les limites de leur mandat, d'accéder aux données introduites dans le SIS et de les consulter.

2. Les membres des équipes du corps européen de garde-frontières et de garde-côtes ou des équipes d'agents impliqués dans les tâches liées aux retours, ainsi que les membres des équipes d'appui à la gestion des flux migratoires accèdent aux données introduites dans le SIS et les consultent, conformément au paragraphe 1, par l'intermédiaire de l'interface technique créée et gérée par l'Agence européenne de garde-frontières et de garde-côtes telle que prévue à l'article 32, paragraphe 2.

3. Lorsqu'il ressort d'une consultation du système par un membre des équipes du corps européen de garde-frontières et de garde-côtes, des équipes d'agents impliqués dans les tâches liées aux retours ou des équipes d'appui à la gestion des flux migratoires qu'il existe un signalement dans le SIS, l'État membre signalant en est informé. Conformément à l'article 40 du règlement (UE) 2016/1624, les membres des équipes ne peuvent agir en réaction à un signalement dans le SIS que sur les instructions et, en règle générale, en présence de garde-frontières ou d'agents impliqués dans les tâches liées au retour de l'État membre hôte dans lequel ils opèrent. L'État membre hôte peut autoriser les membres des équipes à agir en son nom.

4. Chaque accès aux données et chaque consultation effectuée par un membre des équipes du corps européen de garde-frontières et de garde-côtes, des équipes d'agents impliqués dans les tâches liées aux retours ou des équipes d'appui à la gestion des flux migratoires est enregistré dans un journal conformément aux dispositions de l'article 12, de même que toute utilisation qu'il a faite des données auxquelles il a eu accès.

5. L'accès aux données introduites dans le SIS est limité aux membres des équipes du corps européen de garde-frontières et de garde-côtes, des équipes d'agents impliqués dans les tâches liées aux retours et des équipes d'appui à la gestion des flux migratoires et n'est pas accordé aux membres d'autres équipes.

6. Les mesures visant à garantir la sécurité et la confidentialité prévues aux articles 10 et 11 sont adoptées et appliquées.

*Article 32*

*Accès aux données du SIS par l'Agence européenne de garde-frontières et de garde-côtes*

1. Pour l'analyse des menaces susceptibles d'affecter le fonctionnement ou la sécurité des frontières extérieures, l'Agence européenne de garde-frontières et de garde-côtes a le droit d'accéder aux données introduites dans le SIS conformément aux articles 24 et 27, et de les consulter.

2. Aux fins de l'article 31, paragraphe 2, et du paragraphe 1 du présent article, l'Agence européenne de garde-frontières et de garde-côtes crée et gère une interface technique permettant une connexion directe au SIS central.

3. Lorsqu'il ressort d'une consultation du système par l'Agence européenne de garde-frontières et de garde-côtes qu'il existe un signalement dans le SIS, celle-ci en informe l'État membre signalant.

4. Pour l'accomplissement des missions que lui attribue le règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), l'Agence européenne de garde-frontières et de garde-côtes a le droit d'accéder aux données introduites dans le SIS conformément aux articles 24 et 27, et de les vérifier.

5. Lorsqu'il ressort d'une vérification dans le système effectuée par l'Agence européenne de garde-frontières et de garde-côtes, aux fins du paragraphe 2, qu'il existe un signalement dans le SIS, la procédure établie à l'article 22 du règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) s'applique.

6. Aucune disposition du présent article ne doit être interprétée comme affectant les dispositions du règlement (UE) 2016/1624 relatives à la protection des données et à la responsabilité du fait d'un traitement non autorisé ou incorrect de données par l'Agence européenne de garde-frontières et de garde-côtes.

7. Chaque accès aux données et chaque consultation effectuée par l'Agence européenne de garde-frontières et de garde-côtes est enregistré dans un journal conformément aux dispositions de l'article 12, de même que toute utilisation qu'elle a faite des données auxquelles elle a eu accès.

8. Hormis si cela est nécessaire pour l'accomplissement des missions définies aux fins du règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), aucune des parties du SIS ne doit être connectée à un système informatique de collecte et de traitement des données exploité par l'Agence européenne de garde-frontières et de garde-côtes ou en son sein, et aucune des données contenues dans le SIS auxquelles cette agence a accès ne doit être transférée vers un tel système. Aucune partie du SIS ne doit être téléchargée. L'enregistrement dans un journal des accès et des consultations n'est pas considéré comme un téléchargement ou une copie de données du SIS.

9. Les mesures visant à garantir la sécurité et la confidentialité prévues aux articles 10 et 11 sont adoptées et appliquées.

*Article 33*
*Limites d'accès*

Les utilisateurs finaux, y compris Europol, ainsi que l'Agence européenne de garde-frontières et de garde-côtes, ne peuvent accéder qu'aux données qui sont nécessaires à l'accomplissement de leurs missions.

*Article 34*
*Durée de conservation des signalements*

1. Les signalements introduits dans le SIS aux fins du présent règlement ne sont conservés que pendant le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits.

2. Dans les cinq ans à compter de l'introduction d'un signalement dans le SIS, l'État membre signalant examine la nécessité de l'y maintenir.

3. Chaque État membre fixe, s'il y a lieu, des délais d'examen plus courts, conformément à son droit national.

4. Lorsqu'il est clair pour le personnel du bureau SIRENE, chargé de coordonner et de vérifier la qualité des données, que le signalement d'une personne a atteint son objectif et devrait être supprimé du SIS, ce personnel adresse une notification à l'autorité signalante de manière à ce que cette question soit portée à l'attention de celle-ci. L'autorité dispose d'un délai de 30 jours calendrier à compter de la réception de cette notification pour indiquer que le signalement a été ou sera supprimé ou pour exposer les raisons du maintien du signalement. Faute de réponse à l'expiration du délai de 30 jours, le personnel du bureau SIRENE supprime le signalement. Les bureaux SIRENE signalent tout problème récurrent dans ce domaine à leur autorité de contrôle nationale.

5. L'État membre signalant peut, dans le délai d'examen, au terme d'une évaluation individuelle globale, qui est enregistrée, décider de maintenir le signalement si les fins auxquelles le signalement a été introduit l'exigent. Dans ce cas, le paragraphe 2 s'applique également à la prolongation du signalement. Toute prolongation du signalement doit être communiquée au CS-SIS.

6. Les signalements sont automatiquement effacés à l'expiration du délai d'examen visé au paragraphe 2, sauf dans le cas où l'État membre signalant a informé le CS-SIS de la prolongation du signalement conformément au paragraphe 5. Le CS-SIS informe automatiquement les États membres de la suppression programmée de données dans le système moyennant un préavis de quatre mois.

7. Les États membres tiennent des statistiques concernant le nombre de signalements dont la durée de conservation a été prolongée conformément au paragraphe 5.

*Article 35*
*Suppression des signalements*

1. Les signalements aux fins de refus d'entrée et de séjour introduits conformément à l'article 24 sont supprimés lorsque l'autorité compétente a retiré la décision ayant fondé l'introduction du signalement, s'il y a lieu au terme de la procédure de consultation visée à l'article 26.

2. Les signalements relatifs à des ressortissants de pays tiers qui font l'objet d'une mesure restrictive, visés à l'article 27, sont supprimés lorsque la mesure mettant en œuvre l'interdiction de voyage a pris fin, a été suspendue ou a été annulée.

3. Les signalements concernant une personne ayant acquis la citoyenneté d'un État dont les ressortissants jouissent du droit de libre circulation dans l'Union sont supprimés dès que l'État membre signalant apprend, ou est informé en application de l'article 38, que la personne concernée a acquis cette citoyenneté.

# CHAPITRE VIII

## RÈGLES GÉNÉRALES RELATIVES AU TRAITEMENT DES DONNÉES

*Article 36*
*Traitement des données du SIS*

1. Les États membres peuvent traiter les données mentionnées à l'article 20 aux fins d'un refus d'entrée et de séjour sur leur territoire.

2. Les données ne peuvent être copiées qu'à des fins techniques, pour autant que cette copie soit nécessaire aux autorités visées à l'article 29 pour effectuer une consultation directe. Les dispositions du présent règlement s'appliquent à ces copies. Tout État membre s'abstient de copier des données de signalements ou des données complémentaires saisies par un autre État membre, de son N.SIS ou du CS-SIS vers d'autres fichiers de données nationaux.

3. Les copies techniques visées au paragraphe 2 alimentant des bases de données hors ligne ne peuvent être conservées que pour une durée inférieure à 48 heures. Cette durée peut être prolongée dans une situation d'urgence jusqu'à ce que cette situation d'urgence prenne fin.

   Nonobstant le premier alinéa, les copies techniques alimentant des bases de données hors ligne destinées aux autorités chargées de délivrer les visas ne sont pas autorisées, à l'exception des copies faites pour n'être utilisées que dans des situations d'urgence résultant d'une indisponibilité du réseau de plus de vingt-quatre heures.

   Les États membres tiennent à jour un inventaire de ces copies, le mettent à la disposition de leur autorité de contrôle nationale et veillent à ce que ces copies soient conformes aux dispositions du présent règlement, et notamment celles de l'article 10.

4. L'accès aux données est autorisé uniquement dans les limites des compétences des autorités nationales visées à l'article 29 et réservé au personnel dûment autorisé.

5. Tout traitement des informations qui figurent dans le SIS à des fins autres que celles pour lesquelles elles y ont été introduites doit se rapporter à un cas précis et être justifié par la nécessité de prévenir une menace grave imminente pour l'ordre et la sécurité publics, pour des raisons graves de sécurité nationale ou aux fins de la prévention d'une infraction grave. À cet effet, l'autorisation préalable de l'État membre signalant doit être obtenue.

6. Les données concernant des documents relatifs à des personnes, introduites conformément à l'article 38, paragraphe 2, points j) et k), du règlement (UE) 2018/xxx, peuvent être utilisées par les autorités visées à l'article 29, paragraphe 1, point d), conformément à la législation de chaque État membre.

7. Toute utilisation de données non conforme aux paragraphes 1 à 6 est considérée comme un détournement de finalité au regard du droit national de chaque État membre.

8. Chaque État membre communique à l'agence eu-LISA la liste de ses autorités compétentes autorisées à consulter directement les données introduites dans le SIS en application du présent règlement ainsi que tout changement apporté à cette liste. La liste indique, pour chaque autorité, les données qu'elle peut consulter et à quelles fins. L'agence eu-LISA veille à ce que la liste soit publiée chaque année au *Journal officiel de l'Union européenne*.

9. Pour autant que le droit de l'Union ne prévoie pas de dispositions particulières, le droit de chaque État membre est applicable aux données introduites dans son N.SIS.

*Article 37*
*Données du SIS et fichiers nationaux*

1. L'article 36, paragraphe 2, n'affecte pas le droit qu'a un État membre de conserver, dans ses fichiers nationaux, des données du SIS sur la base desquelles la conduite à tenir a été exécutée sur son territoire. Ces données sont conservées dans les fichiers nationaux pour une durée maximale de trois ans, sauf si des dispositions particulières du droit national prévoient une durée de conservation plus longue.

2. L'article 36, paragraphe 2, n'affecte pas le droit qu'a un État membre de conserver, dans ses fichiers nationaux, des données contenues dans un signalement particulier qu'il a lui-même introduit dans le SIS.

*Article 38*
*Information en cas d'inexécution de la conduite à tenir demandée dans un signalement*

Si une conduite à tenir demandée ne peut être exécutée, l'État membre requis en informe directement l'État membre signalant.

*Article 39*
*Qualité des données traitées dans le SIS*

1. Un État membre signalant est responsable de l'exactitude et de l'actualité des données, ainsi que de la licéité de leur introduction dans le SIS.

2. Seul l'État membre signalant est autorisé à modifier, compléter, rectifier, mettre à jour ou supprimer les données qu'il a introduites.

3. Lorsqu'un État membre autre que l'État membre signalant dispose d'indices faisant présumer qu'une donnée est matériellement erronée ou a été stockée illégalement, il en informe l'État membre signalant, par voie d'échange d'informations supplémentaires, dans les meilleurs délais et au plus tard dix jours après avoir relevé ces indices. L'État membre signalant vérifie ce qui lui est communiqué et, s'il y a lieu, corrige ou supprime la donnée sans délai.

4. Lorsque les États membres ne peuvent parvenir à un accord dans un délai de deux mois à compter de la découverte des indices, tels que décrits au paragraphe 3, l'État membre qui n'est pas à l'origine du signalement soumet la question aux autorités de contrôle nationales concernées aux fins de l'adoption d'une décision.

5. Les États membres échangent des informations supplémentaires lorsqu'une personne se plaint de ne pas être celle visée par un signalement. Lorsqu'il ressort des

vérifications qu'il existe effectivement deux personnes différentes, la personne qui s'est plainte est informée des mesures établies à l'article 42.

6. Lorsqu'une personne fait déjà l'objet d'un signalement dans le SIS, l'État membre qui introduit un nouveau signalement se met d'accord avec l'État membre qui a introduit le premier signalement sur l'introduction du signalement. L'accord est trouvé par voie d'échange d'informations supplémentaires.

*Article 40*
*Incidents de sécurité*

1. Tout événement ayant ou pouvant avoir un impact sur la sécurité du SIS et susceptible de causer aux données de celui-ci des dommages ou des pertes est considéré comme un incident de sécurité, en particulier lorsque des données peuvent avoir été consultées sans autorisation ou que la disponibilité, l'intégrité et la confidentialité de données ont été ou peuvent avoir été compromises.

2. Les incidents de sécurité sont gérés de telle sorte qu'une réponse rapide, efficace et idoine y soit apportée.

3. Les États membres informent la Commission, l'agence eu-LISA et le Contrôleur européen de la protection des données des incidents de sécurité. L'agence eu-LISA informe la Commission et le Contrôleur européen de la protection des données des incidents de sécurité.

4. Les informations relatives à un incident de sécurité ayant ou pouvant avoir un impact sur le fonctionnement du SIS dans un État membre ou au sein de l'agence eu-LISA, ou sur la disponibilité, l'intégrité et la confidentialité des données saisies ou envoyées par d'autres États membres, sont communiquées aux États membres et signalées conformément au plan de gestion des incidents fourni par l'agence eu-LISA.

*Article 41*
*Différenciation des personnes présentant des caractéristiques similaires*

Si, lors de l'introduction d'un nouveau signalement, il apparaît qu'il existe déjà dans le SIS une personne correspondant à la même description, la procédure ci-après s'applique:

(a) le bureau SIRENE prend contact avec le service demandeur pour vérifier s'il s'agit ou non de la même personne;

(b) lorsque la vérification fait apparaître que la personne faisant l'objet du nouveau signalement et la personne déjà signalée dans le SIS sont bien une seule et même personne, le bureau SIRENE applique la procédure concernant les signalements multiples visée à l'article 39, paragraphe 6. Lorsque la vérification révèle qu'il s'agit en réalité de deux personnes différentes, le bureau SIRENE valide la demande d'introduction du deuxième signalement, en ajoutant les éléments nécessaires pour éviter toute erreur d'identification.

*Article 42*
*Données complémentaires pour traiter les cas d'usurpation d'identité*

1. Lorsqu'il est possible de confondre la personne effectivement visée par un signalement et une personne dont l'identité a été usurpée, l'État membre signalant ajoute dans le signalement, avec le consentement explicite de la personne dont

l'identité a été usurpée, des données concernant cette dernière afin d'éviter les effets négatifs résultant d'une erreur d'identification.

2. Les données concernant une personne dont l'identité a été usurpée sont exclusivement utilisées pour:

   (a) permettre aux autorités compétentes de distinguer la personne dont l'identité a été usurpée de la personne effectivement visée par le signalement;

   (b) permettre à la personne dont l'identité a été usurpée de prouver son identité et d'établir que celle-ci a été usurpée.

3. Aux fins du présent article, seules les données à caractère personnel ci-après peuvent être introduites dans le SIS et faire l'objet d'un traitement ultérieur:

   (a) le(s) nom(s);

   (b) le(s) prénom(s);

   (c) le(s) nom(s) à la naissance;

   (d) les noms utilisés antérieurement ainsi que les pseudonymes éventuellement enregistrés séparément;

   (e) les signes physiques particuliers, objectifs et inaltérables;

   (f) le lieu de naissance;

   (g) la date de naissance;

   (h) le sexe;

   (i) les images faciales;

   (j) les empreintes digitales;

   (k) la ou les nationalités;

   (l) la catégorie du document d'identité de la personne;

   (m) le pays de délivrance du document d'identité de la personne;

   (n) le(s) numéro(s) du document d'identité de la personne;

   (o) la date de délivrance du document d'identité de la personne;

   (p) l'adresse de la victime;

   (q) le nom du père de la victime;

   (r) le nom de la mère de la victime.

4. Les règles techniques nécessaires pour l'introduction et pour le traitement ultérieur des données mentionnées au paragraphe 3 sont établies au moyen de mesures d'exécution définies et élaborées conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

5. Les données mentionnées au paragraphe 3 sont supprimées en même temps que le signalement correspondant, ou plus tôt lorsque la personne concernée le demande.

6. Seules les autorités disposant d'un droit d'accès au signalement correspondant peuvent accéder aux données mentionnées au paragraphe 3, et ce dans l'unique but d'éviter une erreur d'identification.

*Article 43*
*Mise en relation de signalements*

1. Un État membre peut mettre en relation des signalements qu'il introduit dans le SIS. Cette mise en relation a pour effet d'établir un lien entre deux ou plusieurs signalements.

2. La mise en relation est sans effet sur la conduite particulière à tenir qui est demandée dans chacun des signalements mis en relation, ou sur leur durée de conservation.

3. La mise en relation ne porte pas atteinte aux droits d'accès prévus par le présent règlement. Les autorités ne disposant pas d'un droit d'accès à certaines catégories de signalements ne doivent pas pouvoir prendre connaissance du lien vers un signalement auquel elles n'ont pas accès.

4. Un État membre met en relation des signalements lorsque cela répond à un besoin opérationnel.

5. Lorsqu'un État membre estime que la mise en relation de signalements par un autre État membre n'est pas compatible avec son droit national ou ses obligations internationales, il peut prendre les mesures nécessaires pour faire en sorte que le lien établi ne soit pas accessible à partir de son territoire national ou pour les autorités relevant de sa juridiction établies en dehors de son territoire.

6. Les règles techniques nécessaires pour la mise en relation des signalements sont établies et élaborées conformément à la procédure d'examen définie à l'article 55, paragraphe 2.

*Article 44*
*Objet et durée de conservation des informations supplémentaires*

1. Les États membres conservent au sein du bureau SIRENE une trace des décisions ayant donné lieu à un signalement, afin de faciliter l'échange d'informations supplémentaires.

2. 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 objectifs pour lesquels 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.

3. Le paragraphe 2 n'affecte pas le droit qu'a un État membre de conserver, dans des fichiers nationaux, des données relatives à un signalement particulier que cet État membre a introduit dans le SIS ou à un signalement sur la base duquel une conduite à tenir demandée a été exécutée sur son territoire. Le délai pendant lequel les données peuvent être conservées dans ces fichiers est régi par la législation nationale.

*Article 45*
*Transfert de données à caractère personnel à des tiers*

Les données traitées dans le SIS et les informations supplémentaires connexes au titre du présent règlement ne sont pas transférées à des pays tiers ou à des organisations internationales ni mises à leur disposition.

# CHAPITRE IX

## PROTECTION DES DONNÉES

*Article 46*
*Législation applicable*

1. Le règlement (CE) nº 45/2001 s'applique aux traitements de données à caractère personnel effectués par l'agence eu-LISA au titre du présent règlement.

2. Le règlement (UE) 2016/679 s'applique aux traitements de données à caractère personnel effectués par les autorités visées à l'article 29 du présent règlement, pour autant que les dispositions nationales transposant la directive (UE) 2016/680 ne s'appliquent pas.

3. En ce qui concerne les traitements de données effectués par les autorités nationales compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, les dispositions nationales transposant la directive (UE) 2016/680 s'appliquent.

*Article 47*
*Droit d'accès, de rectification des données inexactes et d'effacement de données stockées illégalement*

1. Le droit de toute personne concernée d'accéder aux données la concernant qui sont introduites dans le SIS et de faire rectifier ou effacer ces données s'exerce dans le respect de la législation de l'État membre auprès duquel elle fait valoir ce droit.

2. Si la législation nationale le prévoit, l'autorité de contrôle nationale décide si des informations doivent être communiquées et par quels moyens.

3. Un État membre autre que celui qui a introduit le signalement ne peut communiquer des informations concernant ces données que s'il a d'abord donné à l'État membre signalant la possibilité de prendre position. Cela se fait par voie d'échange d'informations supplémentaires.

4. Un État membre peut décider de ne pas communiquer des informations à la personne concernée, en tout ou en partie, conformément au droit national, dès lors et aussi longtemps qu'une restriction partielle ou complète de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour:

   (a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;

   (b) éviter de nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales;

   (c) protéger la sécurité publique;

   (d) protéger la sécurité nationale;

   (e) protéger les droits et libertés d'autrui.

5. La personne concernée est informée dans les meilleurs délais et en tout cas au plus tard 60 jours après la date à laquelle elle a demandé à avoir accès à des données, ou plus tôt si la législation nationale prévoit un délai plus court.

6. La personne concernée est informée du suivi donné à l'exercice de son droit de rectification et d'effacement dans les meilleurs délais, et en tout cas au plus tard trois mois après la date à laquelle elle a demandé la rectification ou l'effacement, ou plus tôt si la législation nationale prévoit un délai plus court.

*Article 48*
*Droit à l'information*

1. Les ressortissants de pays tiers qui font l'objet d'un signalement introduit en vertu du présent règlement sont informés conformément aux articles 10 et 11 de la directive 95/46/CE. Cette information est fournie par écrit, avec une copie de la décision nationale, visée à l'article 24, paragraphe 1, qui est à l'origine du signalement, ou une référence à ladite décision.

2. Cette information n'est pas fournie:

(f) lorsque:

i) les données à caractère personnel n'ont pas été obtenues auprès du ressortissant de pays tiers concerné;

et

ii) la communication de l'information se révèle impossible ou implique des efforts disproportionnés;

(g) lorsque le ressortissant de pays tiers concerné a déjà l'information;

(h) lorsque la législation nationale permet de déroger au droit à l'information, en particulier pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou à des fins de prévention et de détection des infractions pénales et d'enquêtes et de poursuites en la matière.

*Article 49*
*Voies de recours*

1. Toute personne peut saisir les juridictions ou les autorités compétentes en vertu du droit national de tout État membre, pour consulter, faire rectifier, supprimer ou effacer des données ou pour obtenir une indemnisation en raison d'un signalement la concernant.

2. Les États membres s'engagent mutuellement à exécuter les décisions définitives rendues par les juridictions ou autorités visées au paragraphe 1, sans préjudice des dispositions de l'article 53.

3. Afin d'obtenir une vue d'ensemble cohérente du fonctionnement des voies des recours, les autorités de contrôle nationales sont invitées à élaborer un système statistique standard pour faire rapport annuellement sur:

(a) le nombre de demandes d'accès présentées par des personnes concernées au responsable du traitement et le nombre de cas où l'accès aux données a été accordé;

(b) le nombre de demandes d'accès présentées par des personnes concernées à l'autorité de contrôle nationale et le nombre de cas où l'accès aux données a été accordé;

(c) le nombre de demandes de rectification de données inexactes et d'effacement de données stockées illégalement présentées au responsable du traitement et le nombre de cas où les données ont été corrigées ou supprimées;

(d) le nombre de demandes de rectification de données inexactes et d'effacement de données stockées illégalement présentées à l'autorité de contrôle nationale;

(e) le nombre d'affaires portées devant les juridictions;

(f) le nombre d'affaires dans lesquelles la juridiction a statué en faveur du demandeur sur tout aspect du dossier;

(g) toute observation relative aux cas de reconnaissance mutuelle de décisions définitives rendues par les juridictions ou les autorités d'autres États membres concernant des signalements d'un État membre signalant.

Les rapports des autorités de contrôle nationales sont transmis par l'intermédiaire du mécanisme de coopération établi à l'article 52.

*Article 50*
*Contrôle du N.SIS*

1. Chaque État membre veille à ce que la ou les autorités de contrôle nationales indépendantes désignées dans chaque État membre et investies des pouvoirs mentionnés au chapitre VI de la directive (UE) 2016/680 ou au chapitre VI du règlement (UE) 2016/679 contrôlent en toute indépendance la licéité du traitement des données à caractère personnel dans le cadre du SIS sur leur territoire et leur transmission à partir de celui-ci, y compris pour ce qui concerne l'échange et le traitement ultérieur d'informations supplémentaires.

2. L'autorité de contrôle nationale veille à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données dans le cadre de son N.SIS, répondant aux normes internationales en matière d'audit. Soit l'audit est effectué par l'autorité de contrôle nationale, soit cette autorité commande directement l'audit à un auditeur indépendant en matière de protection des données. En toutes circonstances, l'autorité de contrôle nationale conserve le contrôle de l'auditeur indépendant et assume la responsabilité des travaux de celui-ci.

3. Les États membres veillent à ce que l'autorité de contrôle nationale dispose des ressources nécessaires pour s'acquitter des tâches qui lui sont confiées par le présent règlement.

*Article 51*
*Contrôle de l'agence eu-LISA*

1. Le Contrôleur européen de la protection des données veille à ce que les activités de traitement des données à caractère personnel exercées par l'agence eu-LISA soient effectuées conformément au présent règlement. Les fonctions et les compétences énumérées aux articles 46 et 47 du règlement (CE) nº 45/2001 s'appliquent en conséquence.

2. Le Contrôleur européen de la protection des données veille à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données à

caractère personnel exercées par l'agence eu-LISA, répondant aux normes internationales d'audit. Un rapport d'audit est communiqué au Parlement européen, au Conseil, à l'agence eu-LISA, à la Commission et aux autorités de contrôle nationales. L'agence eu-LISA se voit offrir la possibilité de formuler des observations avant l'adoption du rapport.

*Article 52*
*Coopération entre les autorités de contrôle nationales et le Contrôleur européen de la protection des données*

1. Les autorités de contrôle nationales et le Contrôleur européen de la protection des données, agissant chacun dans les limites de leurs compétences respectives, coopèrent activement dans le cadre de leurs responsabilités et assurent un contrôle coordonné du SIS.

2. Agissant chacun dans les limites de leurs compétences respectives, ils échangent les informations utiles, s'assistent mutuellement pour mener les audits et inspections, examinent les difficultés d'interprétation ou d'application du présent règlement ou d'autres actes juridiques applicables de l'Union, étudient les problèmes révélés lors de l'exercice du contrôle indépendant ou de l'exercice des droits de la personne concernée, formulent des propositions harmonisées de solutions communes aux éventuels problèmes et assurent la sensibilisation aux droits en matière de protection des données, selon les besoins.

3. Aux fins énoncées au paragraphe 2, les autorités de contrôle nationales et le Contrôleur européen de la protection des données se réunissent au minimum deux fois par an, dans le cadre du comité européen de la protection des données établi par le règlement (UE) 2016/679. Le coût et l'organisation de ces réunions sont à la charge dudit comité. Le règlement intérieur est adopté lors de la première réunion. D'autres méthodes de travail sont mises au point d'un commun accord, selon les besoins.

4. Un rapport d'activités conjoint relatif au contrôle coordonné est transmis tous les deux ans par le comité établi par le règlement (UE) 2016/679 au Parlement européen, au Conseil et à la Commission.

# CHAPITRE X

## RESPONSABILITÉ

*Article 53*
*Responsabilité*

1. Chaque État membre est responsable de tout dommage causé à une personne du fait de l'exploitation du N.SIS. Il en va de même en cas de dommage causé par l'État membre signalant, lorsque ce dernier a introduit des données matériellement erronées ou a stocké des données de manière illicite.

2. Lorsque l'État membre contre lequel une action est intentée n'est pas l'État membre signalant, ce dernier est tenu de rembourser, sur demande, les sommes versées à titre d'indemnisation, à moins que l'utilisation des données par l'État membre demandant le remboursement soit contraire au présent règlement.

3. Lorsque le non-respect, par un État membre, des obligations qui lui incombent en vertu du présent règlement entraîne un dommage pour le SIS, cet État membre en est

tenu responsable, sauf si et dans la mesure où l'agence eu-LISA ou un autre État membre participant au SIS n'a pas pris de mesures raisonnables pour empêcher la survenance du dommage ou pour en atténuer l'effet.

# CHAPITRE XI

## DISPOSITIONS FINALES

*Article 54*
*Suivi et statistiques*

1. L'agence eu-LISA veille à ce que des procédures soient mises en place pour assurer le suivi du le fonctionnement du SIS par rapport aux objectifs fixés, tant en termes de résultats que de rapport coût-efficacité, de sécurité et de qualité de service.

2. Aux fins de la maintenance technique et de l'établissement de rapports et de statistiques, l'agence eu-LISA a accès aux informations nécessaires concernant les opérations de traitement effectuées dans le SIS central.

3. L'agence eu-LISA publie des statistiques journalières, mensuelles et annuelles, présentant le nombre d'enregistrements par catégorie de signalements, le nombre de réponses positives par catégorie de signalements, le nombre de consultations du SIS et le nombre d'accès au SIS aux fins d'introduire, d'actualiser ou de supprimer un signalement, sous forme de totaux et ventilées par État membre, y compris des statistiques sur la procédure de consultation visée à l'article 26. Les statistiques ne contiennent pas de données à caractère personnel. Le rapport statistique annuel est publié.

4. Les États membres ainsi qu'Europol et l'Agence européenne de garde-frontières et de garde-côtes communiquent à l'agence eu-LISA et à la Commission les informations nécessaires pour établir les rapports visés aux paragraphes 7 et 8.

5. L'agence eu-LISA communique aux États membres, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes tout rapport statistique qu'elle produit. Pour contrôler la mise en œuvre des actes juridiques de l'Union, la Commission peut demander à l'agence eu-LISA de fournir d'autres rapports statistiques spécifiques, réguliers ou ponctuels, sur la performance ou l'utilisation du SIS et sur la communication par le canal des bureaux SIRENE.

6. Aux fins des paragraphes 3 à 5 du présent article et de l'article 15, paragraphe 5, l'agence eu-LISA crée, met en œuvre et héberge un fichier central sur ses sites techniques contenant les données mentionnées au paragraphe 3 du présent article et à l'article 15, paragraphe 5, qui ne permette pas l'identification des individus mais permette à la Commission et aux agences mentionnées au paragraphe 5 d'obtenir des rapports et statistiques sur mesure. L'agence eu-LISA accorde aux États membres, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes un accès au fichier central, au moyen d'un accès sécurisé via l'infrastructure de communication, assorti d'un contrôle d'accès et de profils d'utilisateurs spécifiques aux seules fins de l'établissement de rapports et de statistiques.

   Les modalités de fonctionnement du fichier central et les règles de protection et de sécurité des données applicables au fichier sont établies et élaborées au moyen de

mesures d'exécution adoptées conformément à la procédure d'examen visée à l'article 55, paragraphe 2.

7. Deux ans après la mise en service du SIS puis tous les deux ans, l'agence eu-LISA présente au Parlement européen et au Conseil un rapport sur le fonctionnement technique du SIS central et de l'infrastructure de communication, y compris la sécurité offerte, et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres.

8. Trois ans après la mise en service du SIS puis tous les quatre ans, la Commission présente un rapport d'évaluation globale du SIS central et des échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres. Cette évaluation globale comprend un examen des résultats obtenus au regard des objectifs fixés, détermine si les principes de base restent valables, fait le point sur l'application du présent règlement en ce qui concerne le SIS central et sur la sécurité offerte par le SIS central et en tire toutes les conséquences pour le fonctionnement futur. La Commission transmet le rapport d'évaluation au Parlement européen et au Conseil.

*Article 55*
*Procédure de comité*

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

*Article 56*

*Modifications du règlement (UE) nº 515/2014*

Le règlement (UE) nº 515/2014[74] est modifié comme suit:

À l'article 6, le paragraphe 6 suivant est ajouté:

«6. Pendant la phase de développement, les États membres reçoivent en plus de leur enveloppe de base une dotation supplémentaire de 36,8 millions d'EUR, à distribuer par le versement d'une somme forfaitaire, et ils allouent entièrement ce financement aux systèmes nationaux du SIS afin d'assurer leur modernisation rapide et efficace en fonction de la mise en œuvre du SIS central, comme exigé par le [règlement (UE) 2018/...[*] et le règlement (UE) 2018/...[**]].

[*]Règlement 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 (JO...)

[**]Règlement sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières (JO...)».

[74] Règlement (UE) nº 515/2014 du Parlement européen et du Conseil du 16 avril 2014 portant création, dans le cadre du Fonds pour la sécurité intérieure, de l'instrument de soutien financier dans le domaine des frontières extérieures et des visas (JO L 150 du 20.5.2014, p. 143).

*Article 57*
*Abrogation*

Règlement (CE) nº 1987/2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération;

décision 2010/261/UE de la Commission du 4 mai 2010 établissant un plan de sécurité pour le SIS II central et l'infrastructure de communication[75].

Article 25 de la convention d'application de l'accord de Schengen[76].

*Article 58*
*Entrée en vigueur et applicabilité*

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Il s'applique à partir de la date fixée par la Commission après que:

   (a) les mesures d'application nécessaires ont été adoptées;

   (b) 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;

   (c) l'agence eu-LISA a informé la Commission de l'achèvement de toutes les activités de test concernant le CS-SIS et l'interaction entre le CS-SIS et les N.SIS.

3. Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément au traité sur le fonctionnement de l'Union européenne.

Fait à Bruxelles, le

| | |
|---|---|
| *Par le Parlement européen* | *Par le Conseil* |
| *Le président* | *Le président* |

[75] Décision 2010/261/UE de la Commission du 4 mai 2010 établissant un plan de sécurité pour le SIS II central et l'infrastructure de communication (JO L 112 du 5.5.2010, p. 31).

[76] JO L 239 du 22.9.2000, p. 19.

# FICHE FINANCIÈRE LÉGISLATIVE

## 1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB

1.3. Nature de la proposition/de l'initiative

1.4. Objectif(s)

1.5. Justification(s) de la proposition/de l'initiative

1.6. Durée et incidence financière

1.7. Mode(s) de gestion prévu(s)

## 2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système de gestion et de contrôle

2.3. Mesures de prévention des fraudes et irrégularités

## 3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence estimée sur les dépenses

*3.2.1. Synthèse de l'incidence estimée sur les dépenses*

*3.2.2. Incidence estimée sur les crédits opérationnels*

*3.2.3. Incidence estimée sur les crédits de nature administrative*

*3.2.4. Compatibilité avec le cadre financier pluriannuel actuel*

*3.2.5. Participation de tiers au financement*

3.3. Incidence estimée sur les recettes

# FICHE FINANCIÈRE LÉGISLATIVE

## 1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

### 1.1. Dénomination de la proposition/de l'initiative

Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières et abrogeant le règlement (CE) n° 1987/2006.

### 1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB[77]

Domaine politique: Migration et affaires intérieures (Titre 18)

### 1.3. Nature de la proposition/de l'initiative

☐ La proposition/l'initiative porte sur **une action nouvelle**

☐ La proposition/l'initiative porte sur **une action nouvelle suite à un projet pilote/une action préparatoire[78]**

☑ La proposition/l'initiative est relative à **la prolongation d'une action existante**

☐ La proposition/l'initiative porte sur **une action réorientée vers une nouvelle action**

### 1.4. Objectif(s)

*1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition/l'initiative*

Objectif – «Vers une politique nouvelle en matière de migration»

La Commission a insisté, à plusieurs reprises, sur la nécessité de réexaminer la base juridique du SIS afin de s'attaquer aux nouveaux défis qui se posent en matière de sécurité et de migration. Ainsi, dans l'«agenda européen en matière de migration»[79], la Commission déclarait que gérer plus efficacement les frontières impliquait de mieux exploiter les possibilités offertes par les systèmes informatiques et les technologies de l'information. Dans le «programme européen en matière de sécurité»[80], elle annonçait son intention de procéder à une évaluation du SIS en 2015-2016 et d'étudier les possibilités d'aider les États membres à instaurer des interdictions de voyager au niveau national. Dans le «Plan d'action de l'UE contre le trafic de migrants»[81], la Commission indiquait envisager de rendre obligatoire, pour les autorités des États membres, l'enregistrement dans le SIS de toutes les interdictions d'entrée, afin que celles-ci puissent être exécutées sur tout le territoire de l'Union. Elle y déclarait en outre vouloir étudier s'il était possible et proportionné de saisir dans le SIS les décisions en matière de retour rendues par les autorités des États membres pour voir si un migrant en situation irrégulière qu'elles auraient appréhendé fait l'objet, dans un autre État membre, d'une mesure de retour. Enfin, dans sa communication intitulée «Des systèmes d'information plus robustes et plus

---

77 ABM: activity-based management; ABB: activity-based budgeting.

78 Tel(le) que visé(e) à l'article 54, paragraphe 2, point a) ou b), du règlement financier.

79 COM(2015) 240 final.

80 COM(2015) 185 final.

81 COM(2015) 285 final.

intelligents au service des frontières et de la sécurité»[82], la Commission a mentionné tout particulièrement explorer la possibilité d'ajouter des fonctionnalités au SIS dans le cadre de propositions connexes révisant la base juridique de ce système.

À la suite de l'évaluation globale du système et dans le droit fil des objectifs pluriannuels de la Commission, définis dans les communications précitées et dans le plan stratégique pour 2016-2020 de la DG Migration et affaires intérieures[83], la présente proposition vise à réformer la structure, le fonctionnement et l'utilisation du système d'information Schengen dans le domaine des vérifications aux frontières.

*1.4.2. Objectif(s) spécifique(s) et activité(s) ABM/ABB concernée(s)*

Objectif spécifique n°

Plan de gestion 2017 de la DG Migration et affaires intérieures - Objectif spécifique n° 1.2:

Gestion efficace des frontières - sauver des vies et assurer la sécurité des frontières extérieures de l'UE

Activité(s) ABM/ABB concernée(s)

Chapitre 18 02 – Sécurité intérieure

82 COM(2016) 205 final.

83 Ares(2016)2231546 – 12/5/2016.

### *1.4.3. Résultat(s) et incidence(s) attendu(s)*

*Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.*

Les principaux objectifs de l'action sont les suivants:

1). contribuer à un niveau élevé de sécurité au sein de l'espace de liberté, de sécurité et de justice de l'UE;

2) renforcer l'efficacité et l'efficience des contrôles aux frontières.

Dans l'évaluation globale du SIS, qu'elle a effectuée en 2015-2016, la DG Migration et affaires intérieures recommandait d'apporter des améliorations techniques au système et d'harmoniser les procédures nationales dans le domaine de la gestion des refus d'entrée et de séjour. Par exemple, le règlement SIS II en vigueur se borne à autoriser les États membres à introduire dans le système des signalements de refus d'entrée et de séjour. Certains États membres introduisent systématiquement toutes les interdictions d'entrée dans le SIS, d'autres non. Dès lors, la présente proposition contribuera à un degré plus élevé d'harmonisation dans ce domaine en rendant obligatoire la saisie, dans le SIS, de toutes les interdictions d'entrée, et définira des règles communes sur l'introduction des signalements dans le système et précisera le motif sous-jacent de chaque signalement.

La nouvelle proposition instaure des mesures qui répondent aux besoins opérationnels et techniques des utilisateurs finaux. En particulier, de nouveaux champs de données pour les signalements existants permettront aux garde-frontières de disposer de toutes les informations nécessaires pour accomplir efficacement leur mission. En outre, la proposition souligne expressément l'importance que le SIS soit disponible de façon ininterrompue, les temps d'arrêt pouvant avoir des répercussions non négligeables sur la capacité d'effectuer les contrôles aux frontières extérieures. En conséquence, la présente proposition aura un effet particulièrement positif sur l'efficacité des contrôles aux frontières.

Une fois adoptées et mises en œuvre, ces propositions permettront de garantir une plus grande continuité des opérations, puisque les États membres seront tenus de posséder une copie nationale complète ou partielle et une copie de sauvegarde. Le système conservera ainsi tout son caractère fonctionnel et opérationnel pour les agents sur le terrain.

### *1.4.4. Indicateurs de résultats et d'incidences*

*Préciser les indicateurs permettant de suivre la réalisation de la proposition/de l'initiative.*

Pendant la mise à niveau du système

Une fois le projet de proposition approuvé et les spécifications techniques adoptées, le SIS sera mis à niveau afin d'harmoniser davantage les procédures nationales d'utilisation du système, d'élargir la portée du système en amplifiant les volumes d'informations dont pourront disposer les utilisateurs finaux afin de mieux informer les agents procédant aux vérifications, et d'introduire des changements techniques destinés à améliorer la sécurité et à contribuer à réduire les charges administratives. L'agence eu-LISA cordonnera la gestion du projet de mise à niveau du système. Elle instaurera une structure de gestion du projet et fournira un calendrier détaillé assorti des échéances importantes pour la mise en œuvre des changements proposés, ce qui permettra à la Commission de suivre de près la mise en œuvre de la proposition.

Objectif spécifique – Mise en service, en 2020, des fonctionnalités mises à jour du SIS.

Indicateur – Réalisation concluante de tests de pré-lancement complets du système révisé.

Une fois le système opérationnel

Une fois que le système sera opérationnel, l'agence eu-LISA veillera à ce que des procédures soient mises en place pour assurer le suivi du fonctionnement du SIS par rapport aux objectifs fixés en matière de résultats, de coût-efficacité, de sécurité et de qualité du service. Deux ans après la mise en service du SIS puis tous les deux ans, l'agence eu-LISA sera tenue de présenter au Parlement européen et au Conseil un rapport sur le fonctionnement technique du SIS central et de l'infrastructure de communication, y compris la sécurité offerte, et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres. Par ailleurs, l'agence eu-LISA produira des statistiques quotidiennes, mensuelles et annuelles présentant le nombre d'enregistrements dans un journal par catégorie de signalements, le nombre annuel de réponses positives obtenues par catégorie de signalements, le nombre de consultations du SIS et le nombre d'accès au système pour l'introduction, la mise à jour ou la suppression d'un signalement, sous forme de totaux et ventilées par État membre.

Trois ans après la mise en service du SIS puis tous les quatre ans, la Commission présentera un rapport d'évaluation globale du SIS central et des échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres. Cette évaluation globale devra comprendre un examen des résultats obtenus au regard des objectifs fixés, déterminer si les principes de base restent valables, faire le point sur l'application du présent règlement en ce qui concerne le SIS central et sur la sécurité offerte par celui-ci, et en tirer toutes les conséquences pour le fonctionnement futur. La Commission transmettra le rapport d'évaluation au Parlement européen et au Conseil.

## 1.5. Justification(s) de la proposition/de l'initiative

### *1.5.1. Besoin(s) à satisfaire à court ou à long terme*

1. contribuer au maintien d'un niveau élevé de sécurité au sein de l'espace de liberté, de sécurité et de justice de l'UE;

2. renforcer la lutte contre la criminalité internationale, le terrorisme et les autres menaces pour la sécurité;

3. élargir la portée du SIS en ajoutant des éléments nouveaux aux signalements de refus d'entrée et de séjour;

4. accroître l'efficacité des contrôles aux frontières;

5. augmenter l'efficience de l'action des garde-frontières et des services de l'immigration;

6. parvenir à une plus grande efficacité et à une harmonisation plus poussée des procédures nationales et veiller au caractère exécutoire des interdictions d'entrée dans tout l'espace Schengen;

7. contribuer à la lutte contre l'immigration irrégulière.

### *1.5.2. Valeur ajoutée de l'intervention de l'UE*

Le SIS est, en Europe, la principale base de données dans le domaine de la sécurité. En l'absence de contrôles aux frontières intérieures, la lutte effective contre la criminalité et le terrorisme a acquis une dimension européenne. Le SIS est dès lors

indispensable lorsqu'il s'agit d'appuyer les contrôles aux frontières extérieures et les vérifications portant sur les migrants en situation irrégulière trouvés sur le territoire national. Les objectifs de la présente proposition se rapportent à des améliorations techniques destinées à accroître l'efficience et l'efficacité du système et à en harmoniser l'utilisation dans l'ensemble des États membres participants. La nature transnationale de ces objectifs ainsi que le défi consistant à assurer un échange d'informations efficace pour contrer des menaces toujours plus diversifiées impliquent que l'Union est la plus à même de proposer des solutions à ces problèmes. Les objectifs consistant à accroître l'efficience et l'utilisation harmonisée du SIS, à savoir l'augmentation du volume, de la qualité et de la vitesse de l'échange d'informations par l'intermédiaire d'un système d'information à grande échelle centralisé, géré par une agence de régulation (eu-LISA), ne peuvent être réalisés par les seuls États membres et exigent une intervention au niveau de l'Union. Si l'on ne s'emploie pas à résoudre les présentes questions, le SIS continuera de fonctionner selon les règles actuellement applicables, laissant ainsi échapper des possibilités d'optimiser l'efficience et la valeur ajoutée de l'Union, recensées au moyen de l'évaluation du SIS et de son utilisation par les États membres.

Pour la seule année 2015, les autorités nationales ont interrogé le SIS près de 2,9 milliards de fois et ont échangé plus de 1,8 million d'informations supplémentaires, ce qui démontre clairement l'indispensable contribution de celui-ci aux contrôles aux frontières extérieures. Des solutions décentralisées n'auraient pas permis d'atteindre un niveau si élevé d'échange d'informations entre les États membres et il aurait été impossible de parvenir à ces résultats au niveau national. En outre, le SIS s'est révélé être l'outil d'échange d'informations le plus efficace aux fins de la lutte antiterroriste et il apporte de la valeur ajoutée européenne car il permet aux services de sécurité intérieure de coopérer d'une manière rapide, confidentielle et efficiente. Les nouvelles propositions faciliteront davantage l'échange d'informations et la coopération entre les autorités des États membres de l'UE chargées des contrôles aux frontières. Par ailleurs, dans le cadre de leurs compétences respectives, Europol et l'agence européenne de garde-frontières et de garde-côtes se verront accorder un accès total au système, signe manifeste de la valeur ajoutée de l'intervention de l'UE.

*1.5.3. Leçons tirées d'expériences similaires*

Les principales leçons tirées du développement du système d'information Schengen de deuxième génération ont été les suivantes:

1. La phase de développement ne devrait débuter qu'une fois les exigences techniques et opérationnelles entièrement définies. Le développement ne pourra avoir lieu qu'après l'adoption définitive des instruments juridiques sur lesquels il repose et qui exposent sa finalité, sa portée, ses fonctions et ses détails techniques.

2. La Commission a mené (et mène encore) des consultations fréquentes avec les parties intéressées, y compris les délégués auprès du comité SIS-VIS au titre de la procédure de comité. Ce comité est composé de représentants des États membres, à la fois pour les questions opérationnelles SIRENE (coopération transfrontière en relation avec le SIS) et les questions techniques relatives au développement et à la maintenance du SIS et de l'application SIRENE liée. Les changements proposés par le présent règlement ont été discutés de manière transparente et approfondie lors de réunions et d'ateliers qui leur ont été consacrés. Par ailleurs, la Commission a, en interne, institué un groupe de pilotage interservices, comprenant le Secrétariat général et les directions générales de la migration et des affaires intérieures, de la

justice et des consommateurs, des ressources humaines et de la sécurité, et de l'informatique. Ce groupe de pilotage a suivi le processus d'évaluation et émis des orientations lorsque cela était nécessaire.

3. La Commission a également recherché une expertise externe en commandant trois études, dont les résultats ont été intégrés dans l'élaboration de la présente proposition:

- évaluation technique du SIS (Kurt Salmon) – cette évaluation a permis de recenser les principaux problèmes relatifs au SIS et les besoins futurs qu'il conviendrait de prendre en considération; elle a également permis de répertorier des sujets de préoccupation quant au fait d'assurer une continuité maximale des opérations et l'adaptabilité de l'architecture globale à des exigences de capacité croissantes;

- analyse d'impact, sur le plan des technologies de l'information et de la communication, des éventuelles améliorations à apporter à l'architecture du SIS II (Kurt Salmon) – l'étude a apprécié le coût actuel de l'exploitation du SIS au niveau national et évalué trois scénarios techniques possibles pour l'amélioration du système. Les scénarios contiennent tous un ensemble de propositions techniques axées sur les améliorations à apporter au système central et à l'architecture globale;

- Étude sur la faisabilité et les implications de la mise en place, dans le cadre du système d'information Schengen, d'un système permettant, à l'échelle de l'UE, d'échanger des informations sur les décisions de retour et d'en contrôler le respect (PwC) - cette étude apprécie la faisabilité ainsi que les implications techniques et opérationnelles des changements qu'il est proposé d'apporter au SIS aux fins d'en améliorer l'utilisation pour procéder au retour des migrants en situation irrégulière et les empêcher de revenir.

*1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments appropriés*

Il conviendrait de considérer la présente proposition comme la mise en œuvre des mesures énoncées dans la communication du 6 avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité»[84] qui met en avant la nécessité pour l'UE de renforcer et de perfectionner ses systèmes d'information, l'architecture des données et l'échange d'informations en matière répressive, d'antiterrorisme et de gestion des frontières.

De surcroît, la proposition se situe dans la ligne de plusieurs politiques de l'Union menées dans ce domaine:

a) la politique de sécurité intérieure, puisque le SIS contribuera à empêcher l'entrée des ressortissants de pays tiers qui représentent une menace pour la sécurité;

b) la politique de protection des données, dans la mesure où la présente proposition doit garantir la protection des droits fondamentaux pour assurer le respect de la vie privée des personnes dont les données à caractère personnel sont traitées dans le SIS;

La proposition est également compatible avec des actes législatifs de l'Union européenne en vigueur, concernant:

a) une politique de l'Union en matière de retour qui soit efficace, afin de contribuer au système par lequel l'Union détecte et empêche la rentrée sur son territoire de ressortissants de pays tiers ayant fait l'objet d'une mesure de retour, et de le renforcer. Cela contribuera à réduire les incitations à l'immigration irrégulière vers

84 COM(2016) 205 final.

l'UE, ce qui est l'un des principaux objectifs de l'agenda européen en matière de migration[85].b) le **corps européen de garde-frontières et de garde-côtes[86]:** quant à la possibilité pour le personnel de l'agence d'effectuer des analyses des risques ainsi que pour les équipes du corps européen de garde-frontières et de garde-côtes, les équipes d'agents impliqués dans les tâches liées au retour et les membres des équipes d'appui à la gestion des flux migratoires d'avoir accès, dans les limites de leur mandat, au SIS et d'y consulter des données;

c) les **contrôles aux frontières extérieures**, dans la mesure où la présente proposition de règlement vise à aider les différents États membres à contrôler leur tronçon des frontières extérieures de l'Union et, ce faisant, à instaurer la confiance dans l'efficacité du système de l'Union de gestion des frontières;

d) Europol, dans la mesure où la présente proposition prévoit de lui accorder des droits supplémentaires d'accès aux données saisies dans le SIS et de consultation de celles-ci, dans les limites de son mandat;

La proposition est également compatible avec de futurs instruments législatifs de l'Union européenne, en ce qui concerne:

a) le **système d'entrée/sortie[87]**, dans la mesure où la présente proposition vise à refléter l'utilisation combinée d'empreintes digitales et d'images faciales en tant qu'identifiants biométriques aux fins du bon fonctionnement de ce système.

b) l'ETIAS, qui propose de soumettre les ressortissants de pays tiers qui ont l'intention de se rendre dans l'UE et qui sont exemptés de l'obligation de visa à une évaluation complète de sécurité, y compris par une vérification dans le SIS.

85 COM(2015) 240 final.

86 Règlement (UE) 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) n° 863/2007 du Parlement européen et du Conseil, le règlement (CE) n° 2007/2004 du Conseil, et la décision 2005/267/CE du Conseil (JO L 251 du 16.9.2016, p. 1).

87 Proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie (EES) pour enregistrer les données relatives aux entrées et aux sorties des ressortissants de pays tiers qui franchissent les frontières extérieures des États membres de l'Union européenne ainsi que les données relatives aux refus d'entrée les concernant, portant détermination des conditions d'accès à l'EES à des fins répressives et portant modification du règlement (CE) n° 767/2008 et du règlement (UE) n° 1077/2011, COM(2016) 194 final.

## 1.6. Durée et incidence financière

☐ Proposition/initiative à **durée limitée**

– ☐ Proposition/initiative en vigueur à partir de/du [JJ/MM]AAAA jusqu'en/au [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA

☑ Proposition/initiative à **durée illimitée**

– Mise en œuvre avec une période de montée en puissance de 2018 jusqu'en 2020,

– puis un fonctionnement en rythme de croisière au-delà.

## 1.7. Mode(s) de gestion prévu(s)[88]

☑ **Gestion directe** par la Commission

– ☑ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives

☑ **Gestion partagée** avec les États membres

☑ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou aux organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☑ aux organismes visés aux articles 208 et 209 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

La Commission sera chargée de la gestion globale de la politique et l'agence eu-LISA, du développement, du fonctionnement et de la maintenance du système.

**Le SIS constitue un seul système d'information. En conséquence, les dépenses prévues dans deux des propositions du train de mesures considéré [à savoir, la présente proposition et la proposition de règlement 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] ne devraient pas être**

[88] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_fr.html

**considérées comme des montants distincts, mais comme formant un tout. Les incidences budgétaires des modifications nécessaires à la mise en œuvre de ces deux propositions sont exposées dans une seule et même fiche financière législative.**

## 2. MESURES DE GESTION

### 2.1. Dispositions en matière de suivi et de compte rendu

*Préciser la fréquence et les conditions de ces dispositions.*

L'utilisation du SIS fera l'objet d'un examen et d'un suivi réguliers de la part de la Commission, des États membres et de l'agence eu-LISA, qui s'assureront ainsi que le système continue à fonctionner de manière efficace et efficiente. Pour mettre en œuvre les mesures techniques et opérationnelles décrites dans la présente proposition, la Commission sera assistée par le comité.

En outre, l'article 54, paragraphes 7 et 8, du règlement proposé prévoit un processus formel d'examen et d'évaluation réguliers.

Tous les deux ans, l'agence eu-LISA sera tenue de remettre au Parlement européen et au Conseil un rapport sur le fonctionnement technique du SIS, y compris la sécurité offerte, et de l'infrastructure de communication sur laquelle il s'appuie, et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres.

De plus, tous les quatre ans, la Commission devra procéder à une évaluation globale du SIS et des échanges d'informations entre les États membres et la présenter au Parlement européen et au Conseil. Dans ce cadre, le Commission:

a) examinera les résultats atteints par rapport aux objectifs;

b) appréciera si les principes qui sous-tendent le système restent valables;

c) analysera comment le règlement est appliqué au système central;

d) évaluera la sécurité du système central;

e) étudiera les implications pour le fonctionnement futur du système.

### 2.2. En outre, l'agence eu-LISA est, désormais, également tenue de fournir des statistiques journalières, mensuelles et annuelles sur l'utilisation du SIS et d'assurer ainsi un suivi continu du système et de son fonctionnement par rapport aux objectifs. Système de gestion et de contrôle

*2.2.1. Risque(s) identifié(s)*

Les risques suivants ont été recensés:

1. Les difficultés potentielles pour l'agence eu-LISA dans la gestion des évolutions exposées dans la présente proposition parallèlement à d'autres en cours (par exemple, la mise en œuvre du système de l'AFIS dans le SIS) et à des évolutions futures (par exemple, le système d'entrée/sortie, l'ETIAS et la mise à niveau d'Eurodac). On pourrait atténuer ce risque en faisant en sorte que l'agence eu-LISA dispose d'effectifs et de ressources suffisants pour exercer ces missions et assurer la gestion courante du contractant chargé du maintien en état de fonctionnement.

2. Difficultés rencontrées par les États membres:

2.1 Ces difficultés sont essentiellement de nature financière. Par exemple, les propositions législatives prévoient notamment le développement obligatoire d'une copie nationale partielle dans chaque N.SIS II. Les États membres qui n'en auront pas déjà développé une devront effectuer les investissements nécessaires. De même, la mise en œuvre sur le plan national du document de contrôle des interfaces devrait être achevée. Les États membres qui ne se seront pas encore exécutés devront la

provisionner dans les budgets des ministères concernés. On pourrait atténuer ce risque en octroyant aux États membres des fonds de l'UE, provenant par exemple du volet «Frontières» du Fonds pour la sécurité intérieure (FSI).

2.2 Les systèmes nationaux doivent s'aligner sur les exigences au niveau central et les discussions avec les États membres à ce sujet risquent de retarder le développement. Ce risque pourrait être atténué grâce à un engagement précoce auprès des États membres sur cette question afin que des mesures soient prises en temps voulu.

*2.2.2. Informations concernant le système de contrôle interne mis en place*

L'agence eu-LISA est responsable des éléments centraux du SIS. Afin de permettre un meilleur suivi de l'utilisation du SIS, d'analyser les tendances concernant la pression migratoire, la gestion des frontières et les infractions pénales, l'agence eu-LISA devrait être en mesure d'acquérir une capacité de fournir des rapports statistiques aux États membres et à la Commission en recourant aux méthodes les plus modernes.

Les comptes de l'agence eu-LISA seront transmis pour approbation à la Cour des comptes, et soumis à la procédure de décharge. Le service d'audit interne de la Commission effectuera des audits en coopération avec l'auditeur interne de l'agence eu-LISA.

*2.2.3. Estimation du coût-bénéfice des contrôles et évaluation du niveau attendu de risque d'erreur*

S.O.

**2.3. Mesures de prévention des fraudes et irrégularités**

*Préciser les mesures de prévention et de protection existantes ou envisagées.*

Les mesures prévues pour lutter contre la fraude sont exposées à l'article 35 du règlement (UE) n° 1077/2011, qui dispose:

1. Afin de lutter contre la fraude, la corruption et d'autres activités illégales, le règlement (CE) n° 1073/1999 s'applique.

2. L'agence adhère à l'accord interinstitutionnel relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF) et arrête immédiatement les dispositions appropriées applicables à l'ensemble de son personnel.

3. Les décisions de financement et les accords et instruments d'application qui en découlent prévoient expressément que la Cour des comptes et l'OLAF peuvent, au besoin, effectuer des contrôles sur place auprès des bénéficiaires des crédits de l'agence ainsi qu'auprès des agents responsables de l'attribution de ces crédits.

Conformément à cette disposition, la décision du conseil d'administration de l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, relative aux conditions et modalités des enquêtes internes en matière de lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts de l'Union, a été adoptée le 28 juin 2012.

La stratégie de prévention et de détection des fraudes de la DG Migration et affaires intérieures s'appliquera.

## 3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

### 3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

| Rubrique du cadre financier pluriannuel | Ligne budgétaire | Nature de la dépense | Participation | | | |
|---|---|---|---|---|---|---|
| | Rubrique 3 – Sécurité et citoyenneté | CD/CND[89] | de pays AELE[90] | de pays candidats[91] | de pays tiers | au sens de l'article 21, paragraphe 2, point b), du règlement financier |
| | 18.0208 – Système d'information Schengen | C.D. | NON | NON | OUI | NON |
| | 18.020101 – Appuyer la gestion des frontières et soutenir une politique commune des visas pour faciliter les voyages effectués de façon légitime | C.D. | NON | NON | OUI | NON |
| | 18.0207 – Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) | C.D. | NON | NON | OUI | NON |

89 CD = crédits dissociés / CND = crédits non dissociés.

90 AELE: Association européenne de libre-échange.

91 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

## 3.2. Incidence estimée sur les dépenses

### *3.2.1. Synthèse de l'incidence estimée sur les dépenses*

| **Rubrique du cadre financier pluriannuel** | 3 | Sécurité et citoyenneté |
|---|---|---|

| DG Migration et affaires intérieures | | | Année **2018** | Année **2019** | Année **2020** | **TOTAL** |
|---|---|---|---|---|---|---|
| • Crédits opérationnels | | | | | | |
| 18.0208 Système d'information Schengen | Engagements | (1) | 6,234 | 1,854 | 1,854 | **9,942** |
| | Paiements | (2) | 6,234 | 1,854 | 1,854 | **9,942** |
| 18.020101 (Frontières et visas) | Engagements | (1) | | 18,405 | 18,405 | **36,810** |
| | Paiements | (2) | | 18,405 | 18,405 | **36,810** |
| **TOTAL des crédits pour la DG MIGRATION ET AFFAIRES INTÉRIEURES** | Engagements | =1+1a +3 | 6,234 | 20,259 | 20,259 | **46,752** |
| | Paiements | =2+2a +3 | 6,234 | 20,259 | 20,259 | **46,752** |

En Mio EUR (à la 3e décimale)

| **Rubrique du cadre financier pluriannuel** | 3 | Sécurité et citoyenneté |
|---|---|---|

| agence eu-LISA | | | Année **2018** | Année **2019** | Année **2020** | **TOTAL** |
|---|---|---|---|---|---|---|
| • Crédits opérationnels | | | | | | |
| Titre 1: Dépenses de personnel | Engagements | (1) | 0,210 | 0,210 | 0,210 | **0,630** |
| | Paiements | (2) | 0,210 | 0,210 | 0,210 | **0,630** |
| Titre 2: Dépenses d'infrastructure et de fonctionnement | Engagements | (1a) | 0 | 0 | 0 | **0** |
| | Paiements | (2 a) | 0 | 0 | 0 | **0** |
| Titre 3: Dépenses opérationnelles | Engagements | (1a) | 12,893 | 2,051 | 1,982 | **16,926** |
| | Paiements | (2 a) | 2,500 | 7,893 | 4,651 | **15,044** |
| **TOTAL des crédits pour l'agence eu-LISA** | Engagements | =1+1a +3 | 13,103 | 2,261 | 2,192 | **17,556** |
| | Paiements | =2+2a +3 | 2,710 | 8,103 | 4,861 | **15,674** |

*3.2.2. Incidence estimée sur les crédits opérationnels*

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • TOTAL des crédits opérationnels | Engagements | (4) | | | | | | | | |
| | Paiements | (5) | | | | | | | | |
| • TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques | | (6) | | | | | | | | |
| **TOTAL des crédits pour la RUBRIQUE <….>** du cadre financier pluriannuel | Engagements | =4+ 6 | | | | | | | | |
| | Paiements | =5+ 6 | | | | | | | | |

**Si plusieurs rubriques sont concernées par la proposition/l'initiative:**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| • TOTAL des crédits opérationnels | Engagements | (4) | | | | | | | |
| | Paiements | (5) | | | | | | | |
| • TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques | | (6) | | | | | | | |
| **TOTAL des crédits pour les RUBRIQUES 1 à 4** du cadre financier pluriannuel (Montant de référence) | Engagements | =4+ 6 | 19,337 | 22,520 | 22,451 | | | | **64,308** |
| | Paiements | =5+ 6 | 8,944 | 28,362 | 25,120 | | | | **62,426** |

*3.2.3. Incidence estimée sur les crédits de nature administrative*

| **Rubrique du cadre financier pluriannuel** | **5** | «Dépenses administratives» |
|---|---|---|

En millions d'euros (à la 3e décimale)

| | | Année **N** | Année **N+1** | Année **N+2** | Année **N+3** | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| DG: <…….> | | | | | | | | | |
| • Ressources humaines | | | | | | | | | |
| • Autres dépenses administratives | | | | | | | | | |
| **TOTAL DG** <…….> | Crédits | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour la RUBRIQUE 5** du cadre financier pluriannuel | (Total engagements = Total paiements) | | | | | | | | |

En Mio EUR (à la 3e décimale)

| | | Année **N**[92] | Année **N+1** | Année **N+2** | Année **N+3** | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour les RUBRIQUES 1 à 5** du cadre financier pluriannuel | Engagements | | | | | | | | |
| | Paiements | | | | | | | | |

92 L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative.

3.2.3.1. Incidence estimée sur les crédits opérationnels de l'agence eu-LISA

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☑ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

| **Indiquer les objectifs et les réalisations** ⇩ | | | Année **2018** | | Année **2019** | | Année **2020** | | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6) | | | | | | **TOTAL** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **RÉALISATIONS (outputs)** | | | | | | | | | | | | | | | | | |
| | Type[93] | Coût moyen | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre total | Coût total |
| OBJECTIF SPÉCIFIQUE n° 1[94] Développement système central | | | | | | | | | | | | | | | | | | |
| - Contractant | | | 1 | 5,013 | | | | | | | | | | | | | | 5,013 |
| - Logiciels | | | 1 | 4,050 | | | | | | | | | | | | | | 4,050 |
| - Matériel | | | 1 | 3,692 | | | | | | | | | | | | | | 3,692 |
| Sous-total objectif spécifique n° 1 | | | | 12,755 | | | | | | | | | | | | | | 12,755 |
| OBJECTIF SPÉCIFIQUE n° 2 Maintenance système central | | | | | | | | | | | | | | | | | | |
| - Contractant | | | 1 | 0 | 1 | 0,365 | 1 | 0,365 | | | | | | | | | | 0,730 |
| Logiciels | | | 1 | 0 | 1 | 0,810 | 1 | 0,810 | | | | | | | | | | 1,620 |
| Matériel | | | 1 | 0 | 1 | 0,738 | 1 | 0,738 | | | | | | | | | | 1,476 |
| Sous-total objectif spécifique n° 2 | | | | | | 1,913 | | 1,913 | | | | | | | | | | 3,826 |

93 Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

94 Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OBJECTIF SPÉCIFIQUE n° 3 Réunions/Formations | | | | | | | | | | | | | | | | | |
| Activités de formation | 1 | 0,138 | 1 | 0,138 | 1 | 0,069 | | | | | | | | | | | 0,345 |
| Sous-total objectif spécifique n° 3 | | 0,138 | | 0,138 | | 0,069 | | | | | | | | | | | 0,345 |
| **COÛT TOTAL** | | 12,893 | | 2,051 | | 1,982 | | | | | | | | | | | 16,926 |

Crédits d'engagement en millions d'euros (à la 3$^{e}$ décimale)

3.2.3.2. Incidence estimée sur les crédits de la DG MIGRATION ET AFFAIRES INTÉRIEURES

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☑ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

| **Indiquer les objectifs et les réalisations** ⇩ | | | Année **2018** | | Année **2019** | | Année **2020** | | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6) | | | | | | **TOTAL** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **RÉALISATIONS (outputs)** | | | | | | | | | | | | | | | | | |
| | Type[95] | Coût moyen | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre total | Coût total |
| OBJECTIF SPÉCIFIQUE n° 1[96] Développement système national | | | 1 | | 1 | 1,221 | 1 | 1,221 | | | | | | | | | | 2,442 |
| OBJECTIF SPÉCIFIQUE n° 2 Infrastructure | | | 1 | | 1 | 17,184 | 1 | 17,184 | | | | | | | | | | 34,368 |
| **COÛT TOTAL** | | | | | | 18,405 | | 18,405 | | | | | | | | | | 36,810 |

95 Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

96 Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

3.2.3.3. Incidence estimée sur les ressources humaines de l'agence eu-LISA - Synthèse

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative

– ☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En millions d'euros (à la 3e décimale)

| | Année **2018** | Année **2019** | Année **2020** | **TOTAL** |
|---|---|---|---|---|
| Fonctionnaires (grades AD) | | | | |
| Fonctionnaires (grades AST) | | | | |
| Agents contractuels | 0,210 | 0,210 | 0,210 | 0,630 |
| Agents temporaires | | | | |
| Experts nationaux détachés | | | | |
| **TOTAL** | **0,210** | **0,210** | **0,210** | **0,630** |

Le recrutement est prévu pour janvier 2018. L'ensemble du personnel doit être disponible dès le début de l'année 2018 afin de pouvoir entamer en temps voulu la période de développement, en vue d'assurer la mise en service de la refonte du SIS II en 2020. Les trois nouveaux agents contractuels sont nécessaires tant pour la mise en œuvre du projet que pour l'appui opérationnel et la maintenance après le déploiement et la mise en production. Ces ressources seront utilisées pour les finalités suivantes:

- appuyer la mise en œuvre du projet en tant que membres de l'équipe de projet, ce qui recouvre notamment les activités suivantes: la définition des exigences et des spécifications techniques, la coopération avec les États membres et le soutien à ces derniers pendant la mise en œuvre; les mises à jour du document de contrôle d'interface (DCI), le suivi des prestations contractuelles, la distribution de la documentation et les mises à jour, etc.;
- appuyer les activités de transition pour mettre le système en service en coopération avec le contractant [suivi des différentes versions, actualisations du processus opérationnel, sessions de formation (y compris les activités de formation organisées dans les États membres)], etc.;
- soutenir les activités à plus long terme, la définition des spécifications, les formalités préparatoires à l'établissement des contrats en cas de reconfiguration du système (du fait, par exemple, de l'introduction de la reconnaissance d'images) ou en cas de nécessité de modifier le contrat de maintien en état de fonctionnement du nouveau SIS II afin de couvrir des changements supplémentaires (sous l'angle technique et budgétaire);
- mettre en pratique le soutien de second niveau à la suite de la mise en service (MeS), pendant la maintenance continue et l'exploitation.

Il convient de signaler que les trois nouvelles recrues (AC ETP) s'ajouteront aux ressources des équipes internes qui seront également affectées au projet/au suivi contractuel et financier/aux activités opérationnelles. L'engagement d'agents contractuels permettra d'assortir les contrats d'une durée suffisante et de la continuité requise pour assurer la continuité des opérations et le recours aux mêmes personnes spécialisées pour les activités d'appui opérationnel après la conclusion du projet. En outre, les activités d'appui opérationnel rendent nécessaire l'accès à l'environnement de production qui ne peut pas être confié à des contractants ou à du personnel externe.

3.2.3.4. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

*Estimation à exprimer en équivalents temps plein*

| | | Année **N** | Année **N+1** | Année **N+2** | Année **N+3** | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6) | | |
|---|---|---|---|---|---|---|---|---|
| **• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)** | | | | | | | | |
| XX 01 01 01 (au siège et dans les bureaux de représentation de la Commission) | | | | | | | | |
| XX 01 01 02 (en délégation) | | | | | | | | |
| XX 01 05 01 (recherche indirecte) | | | | | | | | |
| 10 01 05 01 (recherche directe) | | | | | | | | |
| **• Personnel externe (en équivalents temps plein: ETP)**[97] | | | | | | | | |
| XX 01 02 01 (AC, END, INT de l'enveloppe globale) | | | | | | | | |
| XX 01 02 02 (AC, AL, END, INT et JED dans les délégations) | | | | | | | | |
| **XX** 01 04 **yy** [98] | - au siège | | | | | | | |
| | - en délégation | | | | | | | |
| **XX** 01 05 02 (AC, END, INT sur recherche indirecte) | | | | | | | | |
| 10 01 05 02 (AC, END, INT sur recherche directe) | | | | | | | | |
| Autres lignes budgétaires (à préciser) | | | | | | | | |
| **TOTAL** | | | | | | | | |

**XX** est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

| | |
|---|---|
| Fonctionnaires et agents temporaires | |
| Personnel externe | |

97 AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JED = jeune expert en délégation.

98 Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

*3.2.4. Compatibilité avec le cadre financier pluriannuel actuel*

– ☐ La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

– ☑ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

Une reprogrammation du solde de l'enveloppe «frontières intelligentes» du Fonds pour la sécurité intérieure est planifiée, pour permettre la mise en œuvre des fonctionnalités et des changements prévus dans les deux propositions. Le règlement FSI-Frontières est l'instrument financier dans lequel le budget consacré à la mise en œuvre du train de mesures «frontières intelligentes» a été inclus. Son article 5 prévoit que 791 millions d'EUR doivent être consacrés à un programme pour la mise en place de systèmes informatiques permettant la gestion des flux migratoires aux frontières extérieures, dans les conditions énoncées à l'article 15. Sur ces 791 millions d'EUR, 480 millions d'EUR sont réservés au développement du système d'entrée/sortie et 210 millions d'EUR, au développement du système européen d'information et d'autorisation concernant les voyages (ETIAS). Le solde, soit 100,828 millions d'EUR, servira partiellement à financer les coûts induits par les changements prévus dans les deux propositions.

– ☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

*3.2.5. Participation de tiers au financement*

– ☑La proposition/l'initiative ne prévoit pas de cofinancement par des tierces parties.

– La proposition/l'initiative prévoit un cofinancement estimé ci-après:

Crédits en millions d'euros (à la 3e décimale)

| | Année **N** | Année **N+1** | Année **N+2** | Année **N+3** | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6) | | | Total |
|---|---|---|---|---|---|---|---|---|
| Préciser l'organisme de cofinancement | | | | | | | | |
| TOTAL crédits cofinancés | | | | | | | | |

### 3.3. Incidence estimée sur les recettes

– ☐ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☑ La proposition/l'initiative a une incidence financière décrite ci-après:

– ☐ sur les ressources propres

– ☑ sur les recettes diverses

En millions d'euros (à la 3e décimale)

| Ligne budgétaire de recettes: | Montants inscrits pour l'exercice en cours | Incidence de la proposition/de l'initiative[99] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 2018 | 2019 | 2020 | 2021 | Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6) | | |
| Article 6313 – contribution des pays associés à l'espace Schengen (CH, NO, LI et IS). | | p.m | p.m | p.m | p.m | | | |

Pour les recettes diverses qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépense concernée(s).

18.02.08 (Système d'information Schengen), 18.02.07 (agence eu-LISA)

Préciser la méthode de calcul de l'incidence sur les recettes.

Le budget comprendra une contribution financière des pays associés à la mise en œuvre, à l'application et au développement de l'acquis de Schengen.

[99] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 25 % de frais de perception.