RÈGLEMENT (UE) 2018/1861 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 28 novembre 2018

sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) nº 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 ([1]),

considérant ce qui suit:

(1) Le système d'information Schengen (SIS) constitue un outil essentiel pour l'application des dispositions de l'acquis de Schengen tel qu'il a été 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 par le soutien qu'il apporte à la coopération opérationnelle entre les autorités nationales compétentes, notamment les garde-frontières, les services de police, les autorités douanières, les autorités chargées de l'immigration et les autorités chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes et poursuites en la matière ou de l'exécution des sanctions pénales.

(2) Le SIS a initialement été créé en vertu des 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 ([2]) (ci-après dénommée «convention d'application de l'accord de Schengen»), signée le 19 juin 1990. La Commission a été chargée, par le règlement (CE) nº 2424/2001 du Conseil ([3]) et la décision 2001/886/JAI du Conseil ([4]), du développement du SIS de deuxième génération (SIS II). Il a ultérieurement été créé par le règlement (CE) nº 1987/2006 du Parlement européen et du Conseil ([5]) et par la décision 2007/533/JAI du Conseil ([6]). Le SIS II a remplacé le SIS tel qu'il a été créé par la convention d'application de l'accord Schengen.

(3) Trois ans après l'entrée en service du SIS II, la Commission a procédé à une évaluation du système, conformément au règlement (CE) nº 1987/2006 et à la décision 2007/533/JAI. Le 21 décembre 2016, la Commission a présenté au Parlement européen et au Conseil le rapport d'évaluation du système d'information de Schengen de deuxième génération (SIS II) conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) nº 1987/2006, et à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI, accompagné d'un document de travail des services. Les recommandations formulées dans ces documents devraient être prises en compte, le cas échéant, dans le présent règlement.

(4) Le présent règlement constitue la base juridique pour le SIS dans les domaines relevant du champ d'application de la troisième partie, titre V, chapitre 2, du traité sur le fonctionnement de l'Union européenne. Le règlement (UE) 2018/1862 du Parlement européen et du Conseil ([7]) constitue la base juridique pour le SIS dans les domaines relevant du champ d'application de la troisième partie, titre V, chapitres 4 et 5, du traité sur le fonctionnement de l'Union européenne.

([1]) Position du Parlement européen du 24 octobre 2018 (non encore parue au Journal officiel) et décision du Conseil du 19 novembre 2018.
([2]) JO L 239 du 22.9.2000, p. 19.
([3]) Règlement (CE) nº 2424/2001 du Conseil du 6 décembre 2001 relatif au développement du système d'information Schengen de deuxième génération (SIS II) (JO L 328 du 13.12.2001, p. 4).
([4]) 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).
([5]) Règlement (CE) nº 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).
([6]) 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).
([7]) Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (voir page 56 du présent Journal officiel).

(5) Le fait que la base juridique pour 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. Il devrait comprendre un réseau unique de bureaux nationaux, dénommés bureaux SIRENE, pour assurer l'échange d'informations supplémentaires. Certaines dispositions de ces instruments devraient donc être identiques.

(6) Il est nécessaire de préciser les objectifs du SIS, certains éléments de son architecture technique et de son financement, de fixer des règles concernant son fonctionnement et son utilisation de bout en bout et de définir les responsabilités. Il est également nécessaire de déterminer les catégories de données à introduire dans le système, les finalités de leur introduction et de leur traitement, ainsi que les critères pour leur introduction. Des règles sont également nécessaires pour régir la suppression des signalements, les autorités autorisées à avoir accès aux données et l'utilisation de données biométriques, et pour préciser les obligations en matière de protection des données et de traitement des données.

(7) Les signalements dans le SIS ne contiennent que les informations nécessaires pour identifier une personne et déterminer la conduite à tenir. Par conséquent, il convient que les États membres échangent des informations supplémentaires liées aux signalements lorsque c'est nécessaire.

(8) Le SIS comprend un système central (SIS central) et des systèmes nationaux. Les systèmes nationaux pourraient contenir une copie intégrale ou partielle de la base de données du SIS, qui peut être partagée par deux États membres ou plus. Étant donné que le SIS est l'instrument d'échange d'informations le plus important en Europe pour assurer la sécurité et une gestion efficace des frontières, il est nécessaire de garantir son fonctionnement continu au niveau tant central que national. La disponibilité du SIS devrait faire l'objet d'un suivi étroit au niveau central et des États membres, et tout cas d'indisponibilité pour les utilisateurs finaux devrait être consigné et signalé aux parties intéressées au niveau national et de l'Union. Chaque État membre devrait mettre en place un dispositif de secours pour son système national. Les États membres devraient également garantir une connectivité continue avec le SIS central en prévoyant des points de connexion doubles et physiquement et géographiquement séparés. Il convient de gérer le SIS central et l'infrastructure de communication de manière à assurer leur fonctionnement 24 heures sur 24, 7 jours sur 7. Pour cette raison, l'agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (ci-après dénommée «eu-LISA») créée par le règlement (UE) 2018/1726 du Parlement européen et du Conseil ([1]) devrait mettre en œuvre des solutions techniques pour renforcer la disponibilité continue du SIS, sous réserve d'une analyse d'impact indépendante et d'une analyse coûts/avantages.

(9) 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 (ci-après dénommé «manuel SIRENE»). Les bureaux SIRENE devraient assurer cet échange d'informations de manière rapide et efficace.

(10) Pour garantir un échange efficace d'informations supplémentaires, y compris en ce qui concerne la conduite à tenir spécifiée dans les signalements, il y a lieu de renforcer le fonctionnement des bureaux SIRENE en précisant les exigences quant aux ressources disponibles et à la formation des utilisateurs et au délai pour répondre aux demandes de renseignements reçues d'autres bureaux SIRENE.

(11) Il convient que les États membres veillent à ce que le personnel de leur bureau SIRENE ait les compétences linguistiques et les connaissances du droit et des règles de procédure applicables nécessaires à l'exercice de ses fonctions.

(12) Afin d'être en mesure de bénéficier pleinement des fonctionnalités du SIS, les États membres devraient veiller à ce que les utilisateurs finaux et le personnel des bureaux SIRENE reçoivent régulièrement des formations, portant notamment sur la sécurité des données, la protection des données et la qualité des données. Les bureaux SIRENE devraient être associés à l'élaboration des programmes de formation. Dans la mesure du possible, les bureaux SIRENE devraient en outre prévoir des échanges de personnel avec d'autres bureaux SIRENE au moins une fois par an. Les États membres sont encouragés à prendre les mesures utiles pour empêcher que la rotation du personnel ne cause une perte de compétences et d'expérience.

(13) L'eu-LISA est chargée de la gestion opérationnelle des éléments centraux du SIS. Afin de permettre à l'eu-LISA de consacrer les moyens financiers et humains nécessaires pour couvrir tous les aspects de la gestion opérationnelle du SIS central et de l'infrastructure de communication, le présent règlement devrait décrire ses tâches en détail, notamment en ce qui concerne les aspects techniques de l'échange d'informations supplémentaires.

(14) Sans préjudice de la responsabilité des États membres relative à l'exactitude des données introduites dans le SIS et du rôle des bureaux SIRENE en tant que coordinateurs de la qualité, l'eu-LISA devrait être chargée de renforcer la qualité des données en introduisant un outil de contrôle central de cette qualité et devrait présenter des rapports à

([1]) Règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union 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), modifiant le règlement (CE) n° 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) n° 1077/2011 (JO L 295 du 21.11.2018, p. 99).

la Commission et aux États membres à intervalles réguliers. La Commission devrait faire rapport au Parlement européen et au Conseil sur les problèmes rencontrés quant à la qualité des données. En vue d'améliorer davantage la qualité des données dans le SIS, l'eu-LISA devrait également proposer une formation sur l'utilisation du SIS aux organismes de formation nationaux et, dans la mesure du possible, aux bureaux SIRENE et aux utilisateurs finaux.

(15) En vue d'un meilleur contrôle de l'utilisation du SIS et pour analyser les tendances en matière de pression migratoire et de gestion des frontières, l'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, au Parlement européen, au Conseil, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes sans compromettre l'intégrité des données. Il convient dès lors de créer un fichier central. Les statistiques conservées dans ce fichier ou fournies par celui-ci ne devraient contenir aucune donnée à caractère personnel. Les États membres devraient communiquer, dans le cadre de la coopération entre les autorités de contrôle et le Contrôleur européen de la protection des données prévue par le présent règlement, des statistiques concernant l'exercice du droit d'accès, de rectification des données inexactes et d'effacement des données conservées de manière illicite.

(16) De nouvelles catégories de données devraient être introduites dans le SIS 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 non-admission et d'interdiction 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, lorsqu'une telle information est disponible, une référence au document d'identification personnel de la personne concernée ou au numéro de ce document et une copie du document, si possible en couleurs.

(17) Les autorités compétentes devraient pouvoir, en cas de nécessité absolue, introduire dans le SIS des informations spécifiques concernant des caractéristiques physiques, spécifiques et objectives d'une personne qui ne sont pas susceptibles de changer, telles que des tatouages, des marques ou des cicatrices.

(18) Si elles sont disponibles, toutes les données pertinentes, en particulier le prénom de la personne concernée, devraient être insérées lors de la création d'un signalement, afin de réduire autant que possible le risque de fausses réponses positives et les activités opérationnelles inutiles.

(19) Aucune donnée ayant servi à effectuer des recherches ne devrait être conservée dans le SIS, à l'exception de la tenue de registres afin de pouvoir contrôler la licéité de la recherche et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement des systèmes nationaux, et de garantir l'intégrité et la sécurité des données.

(20) Le SIS devrait permettre le traitement des données biométriques afin d'aider à identifier les personnes concernées de manière fiable. Toute introduction de photographies, d'images faciales ou de données dactyloscopiques dans le SIS et toute utilisation de ces données devraient être limitées à ce qui est nécessaire pour atteindre les objectifs poursuivis, devraient être autorisées par le droit de l'Union, devraient respecter les droits fondamentaux, notamment l'intérêt supérieur de l'enfant, et devraient être conformes au droit de l'Union en matière de protection des données, y compris les dispositions applicables en matière de protection des données prévues par le présent règlement. Dans la même optique, de manière à éviter les problèmes causés par des erreurs d'identification, le SIS devrait également permettre le traitement de données relatives à des personnes dont l'identité a été usurpée, sous réserve de garanties adaptées, de l'obtention du consentement des personnes concernées pour chaque catégorie de données, en particulier les empreintes palmaires, et d'une stricte limitation des fins auxquelles ces données à caractère personnel peuvent être traitées de manière licite.

(21) Les États membres devraient prendre les mesures techniques nécessaires pour que, chaque fois que les utilisateurs finaux ont le droit d'effectuer des recherches dans une base de données nationale des services de police ou d'immigration, ils puissent aussi faire des recherches dans le SIS en parallèle, sous réserve des principes énoncés à l'article 4 de la directive (UE) 2016/680 du Parlement européen et du Conseil [1] et à l'article 5 du règlement (UE) 2016/679 du Parlement européen et du Conseil [2]. Ceci devrait garantir que le SIS fonctionne comme la principale mesure compensatoire dans l'espace sans contrôles aux frontières intérieures et tienne mieux compte de la dimension transfrontière de la criminalité et de la mobilité des criminels.

(22) Le présent règlement devrait définir les conditions d'utilisation des données dactyloscopiques, des photographies et des images faciales à des fins d'identification et de vérification. Les images faciales et les photographies ne devraient être utilisées, dans un premier temps, à des fins d'identification que dans le contexte des points de passage frontalier habituels. Une telle utilisation devrait faire l'objet d'un rapport de la Commission confirmant que la technique requise est disponible, fiable et prête à être employée.

---

[1] 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).

[2] 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).

(23) Les recherches dans les données dactyloscopiques conservées dans le SIS devraient être autorisées à l'aide de séries complètes ou incomplètes d'empreintes digitales ou d'empreintes palmaires trouvées sur le lieu d'une infraction 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, pour autant qu'une recherche soit effectuée simultanément dans les bases de données d'empreintes digitales nationales pertinentes. Il convient d'accorder une attention particulière à l'établissement de normes de qualité applicables à la conservation de données biométriques.

(24) Chaque fois que l'identité d'une personne ne peut être établie par aucun autre moyen, il convient d'utiliser les données dactyloscopiques pour tenter d'identifier la personne. Il devrait être autorisé dans tous les cas d'identifier une personne en utilisant des données dactyloscopiques.

(25) Il devrait être possible pour les États membres de mettre en relation les signalements dans le SIS. Cette mise en relation de deux signalements ou plus ne devrait avoir aucun effet sur la conduite à tenir, le délai de réexamen des signalements ou les droits d'accès aux signalements.

(26) 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 délivrées par les autorités nationales compétentes conformément à des procédures respectant la directive 2008/115/CE du Parlement européen et du Conseil ([1]), et si l'on établit des règles communes pour l'introduction de signalements aux fins de non-admission et d'interdiction de séjour au moment du retour d'un 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 concerné quitte l'espace Schengen et l'activation du signalement dans le SIS. Cela devrait garantir l'application des interdictions d'entrée aux points de passage des frontières extérieures, en empêchant effectivement toute nouvelle entrée dans l'espace Schengen.

(27) Les personnes à l'égard desquelles une décision de non-admission et d'interdiction de séjour a été prise devraient avoir le droit de former un recours contre ladite décision. Il convient que ce droit de recours respecte la directive 2008/115/CE dans le cas d'une décision liée au retour.

(28) Le présent règlement devrait établir des règles obligatoires prévoyant que les autorités nationales sont consultées et qu'une notification leur est adressée lorsqu'un ressortissant de pays tiers est titulaire d'un titre de séjour ou d'un visa de long séjour en cours de validité accordé dans un État membre, ou qu'il est susceptible d'en obtenir un, et qu'un autre État membre envisage d'introduire ou a déjà introduit un signalement aux fins de non-admission et d'interdiction de séjour de ce ressortissant de pays tiers. De telles situations créent en effet de graves incertitudes pour les garde-frontières, les services de 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 de garantir que les ressortissants de pays tiers qui sont autorisés à résider légalement sur le territoire des États membres puissent y entrer sans difficulté et que ceux qui ne sont pas autorisés à entrer en soient empêchés.

(29) Lorsque, à la suite d'une consultation entre États membres, l'État membre signalant supprime un signalement dans le SIS, il devrait pouvoir maintenir l'inscription du ressortissant de pays tiers en question sur sa liste de signalements nationale.

(30) Le présent règlement devrait s'entendre sans préjudice de l'application de la directive 2004/38/CE du Parlement européen et du Conseil ([2]).

(31) Les signalements ne devraient pas être conservés dans le SIS pour une durée plus longue que le temps nécessaire à la réalisation des finalités spécifiques pour lesquelles ils ont été introduits. Dans un délai de trois ans à compter de l'introduction d'un signalement dans le SIS, l'État membre signalant devrait réexaminer la nécessité de le conserver. Cependant, dans le cas où la décision nationale sur laquelle le signalement se fonde prévoit une durée de validité supérieure à trois ans, il convient que le signalement soit réexaminé dans un délai de cinq ans. La décision de conserver des signalements concernant des personnes devrait être fondée sur une évaluation individuelle complète. Les États membres devraient réexaminer les signalements concernant des personnes dans le délai de réexamen prescrit et tenir des statistiques sur le nombre de signalements concernant des personnes dont la durée de conservation a été prolongée.

(32) Lors de l'introduction d'un signalement dans le SIS et du report de la date d'expiration d'un signalement dans le SIS, il convient de respecter une exigence de proportionnalité, impliquant de vérifier si un cas déterminé est suffisamment approprié, pertinent et important pour justifier l'introduction d'un signalement dans le SIS. Dans les cas d'infractions terroristes, le cas devrait être jugé suffisamment approprié, pertinent et important pour justifier un signalement dans le SIS. Pour des raisons de sécurité publique ou nationale, les États membres devraient être autorisés, à titre exceptionnel, à s'abstenir d'introduire un signalement dans le SIS si celui-ci risque de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires.

([1]) 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).

([2]) 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, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO L 158 du 30.4.2004, p. 77).

(33) 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 prévues par le présent règlement et soumises à une procédure uniforme de déclaration des incidents. Leur personnel devrait avoir reçu une formation adéquate et être informé des infractions et sanctions éventuelles en la matière.

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

(35) Afin de renforcer l'efficacité du travail des autorités chargées de l'immigration lorsqu'elles statuent sur le droit de ressortissants de pays tiers d'entrer et de séjourner sur le territoire des États membres, ainsi que sur le retour de ressortissants de pays tiers en séjour irrégulier, il convient de donner à ces autorités un accès au SIS en vertu du présent règlement.

(36) Sans préjudice de règles plus spécifiques prévues par le présent règlement en ce qui concerne le traitement de données à caractère personnel, le règlement (UE) 2016/679 devrait s'appliquer aux traitements de données à caractère personnel effectués par les États membres en vertu du présent règlement, sauf si ces traitements sont effectués par les autorités nationales compétentes aux fins de la prévention et de la détection d'infractions terroristes ou d'autres infractions pénales graves, et des enquêtes et poursuites en la matière.

(37) Sans préjudice de règles plus spécifiques prévues par le présent règlement, les dispositions législatives, réglementaires et administratives nationales adoptées en vertu de la directive (UE) 2016/680 devraient s'appliquer aux traitements de données à caractère personnel effectués en vertu du présent règlement par les autorités nationales compétentes aux fins de la prévention et de la détection d'infractions terroristes ou d'autres infractions pénales graves, des enquêtes et poursuites en la matière ou de l'exécution des sanctions pénales. L'accès aux données introduites dans le SIS et le droit d'effectuer des recherches dans ces données dont disposent les autorités nationales compétentes chargées de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, des enquêtes et poursuites en la matière ou de l'exécution des sanctions pénales sont soumis à toutes les dispositions pertinentes du présent règlement et de la directive (UE) 2016/680 telle qu'elle est transposée en droit national, et en particulier à la surveillance par les autorités de contrôle visées dans la directive (UE) 2016/680.

(38) Le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([1]) 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 au titre du présent règlement.

(39) Le règlement (UE) 2016/794 du Parlement européen et du Conseil ([2]) devrait s'appliquer aux traitements de données à caractère personnel effectués par Europol au titre du présent règlement.

(40) Lorsqu'elles utilisent le SIS, les autorités compétentes devraient veiller au respect de la dignité et de l'intégrité des personnes dont les données sont traitées. Les traitements de données à caractère personnel aux fins du présent règlement ne doivent aboutir à aucune discrimination à l'encontre des personnes, fondée notamment sur le sexe, l'origine raciale ou ethnique, la religion ou les croyances, le handicap, l'âge ou l'orientation sexuelle.

(41) En ce qui concerne la confidentialité, les dispositions pertinentes du statut des fonctionnaires de l'Union européenne et du régime applicable aux autres agents de l'Union fixées dans le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil ([3]) (ci-après dénommés «statut») devraient s'appliquer aux fonctionnaires et autres agents employés et travaillant dans le cadre du SIS.

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

(43) Les autorités de contrôle indépendantes nationales visées dans le règlement (UE) 2016/679 et la directive (UE) 2016/680 (ci-après dénommées «autorités de contrôle») devraient vérifier la licéité des traitements de données à caractère personnel effectués par les États membres en vertu du présent règlement, y compris les échanges d'informations supplémentaires. Les autorités de contrôle devraient être dotées de ressources suffisantes pour mener à bien cette mission. Il convient de prévoir des dispositions sur le droit des personnes concernées d'avoir accès à leurs données à caractère personnel conservées dans le SIS et d'obtenir la rectification et l'effacement de ces données, et sur tout recours ultérieur devant les juridictions nationales ainsi que sur la reconnaissance mutuelle des décisions judiciaires. Il y a également lieu d'imposer aux États membres l'établissement de statistiques annuelles.

([1]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

([2]) 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 24.5.2016, p. 53).

([3]) JO L 56 du 4.3.1968, p. 1.

(44) Les autorités de contrôle devraient veiller à ce que soit réalisé, tous les quatre ans au minimum, un audit des opérations de traitement des données dans les systèmes nationaux de leur État membre, conformément aux normes internationales d'audit. Cet audit devrait être réalisé par les autorités de contrôle elles-mêmes ou être commandé directement par les autorités de contrôle à un auditeur indépendant en matière de protection des données. Ce dernier devrait rester sous le contrôle et la responsabilité des autorités de contrôle concernées, qui devraient dès lors donner des instructions à l'auditeur et définir clairement l'objet de l'audit, son étendue et sa méthode, et donner des indications et exercer un contrôle sur l'audit et ses résultats finaux.

(45) Le Contrôleur européen de la protection des données devrait contrôler les activités des institutions et des organes de l'Union dans le domaine du traitement de données à caractère personnel effectué au titre du présent règlement. Le Contrôleur européen de la protection des données et les autorités de contrôle devraient coopérer dans le cadre du suivi du SIS.

(46) Le Contrôleur européen de la protection des données devrait être doté de ressources suffisantes pour s'acquitter des tâches que lui confie le présent règlement, y compris l'aide de personnes ayant une expertise en matière de données biométriques.

(47) Le règlement (UE) 2016/794 prévoit qu'Europol appuie et renforce l'action des autorités nationales compétentes et leur coopération mutuelle dans la lutte contre le terrorisme et les formes graves de criminalité, et qu'il fournit des analyses et des évaluations de la menace. Afin d'aider Europol à s'acquitter de ses missions, en particulier au sein du Centre européen chargé de lutter contre le trafic de migrants, il convient de permettre à Europol d'avoir accès aux catégories de signalements prévues dans le présent règlement.

(48) 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 sont encouragés à partager avec Europol leurs informations sur les activités liées au terrorisme. Ce partage d'informations devrait s'effectuer par la voie d'échange d'informations supplémentaires avec Europol sur les signalements concernés. À cette fin, Europol devrait établir une connexion avec l'infrastructure de communication.

(49) Il est également nécessaire d'établir des règles claires à l'intention d'Europol au sujet du traitement et du téléchargement des données du SIS pour lui permettre d'utiliser le SIS de manière complète, à condition que les normes en matière de protection des données soient respectées comme le prévoient le présent règlement et le règlement (UE) 2016/794. Lorsque des recherches effectuées dans le SIS par Europol révèlent l'existence d'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, par la voie d'échange d'informations supplémentaires avec le bureau SIRENE concerné, pour permettre à cet État membre de donner suite à l'affaire.

(50) Le règlement (UE) 2016/1624 du Parlement européen et du Conseil [1] prévoit, aux fins dudit règlement, que l'État membre hôte autorise les membres des équipes visés à l'article 2, point 8), dudit règlement qui sont déployés par l'Agence européenne de garde-frontières et de garde-côtes à consulter les bases de données de l'Union lorsque cette consultation est nécessaire à la réalisation des objectifs opérationnels précisés dans le plan opérationnel relatif aux vérifications aux frontières, à la surveillance des frontières et au retour. D'autres agences concernées de l'Union, 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 des équipes visées à l'article 2, points 8) et 9), dudit règlement 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, les équipes visées à l'article 2, points 8) et 9), dudit règlement ont besoin d'avoir accès au SIS par l'intermédiaire d'une interface technique de l'Agence européenne de garde-frontières et de garde-côtes qui permet de se connecter au SIS central. Lorsque des recherches effectuées dans le SIS par les équipes visées à l'article 2, points 8) et 9), du règlement (UE) 2016/1624 ou par les équipes d'agents révèlent l'existence d'un signalement introduit par un État membre, le membre de l'équipe ou l'agent ne peut exécuter la conduite requise que si l'État membre hôte l'y autorise. L'État membre hôte devrait dès lors être informé pour lui permettre de donner suite à l'affaire. L'État membre hôte devrait notifier la réponse positive à l'État membre signalant par la voie d'échange d'informations supplémentaires.

(51) Certains aspects du SIS ne peuvent pas être couverts de manière exhaustive par le présent règlement en raison de leur nature technique, de leur niveau élevé de précision et de leur nature sujette à de fréquents changements. Ces aspects incluent, par exemple, des règles techniques concernant l'introduction, la mise à jour et la suppression des

[1] 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) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil (JO L 251 du 16.9.2016, p. 1).

données, et, les recherches dans les données, et concernant la qualité des données, et des règles liées aux données biométriques, des règles sur la compatibilité et l'ordre de priorité des signalements, sur la mise en relation des signalements, et sur l'échange d'informations supplémentaires. Il convient de conférer des compétences d'exécution relatives à ces aspects à la Commission. Les règles techniques concernant les recherches de signalements devraient tenir compte du bon fonctionnement des applications nationales.

(52) 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) nº 182/2011 du Parlement européen et du Conseil ([1]). La procédure d'adoption des actes d'exécution au titre du présent règlement et du règlement (UE) 2018/1862 devrait être identique.

(53) Pour assurer la transparence, l'eu-LISA devrait, deux ans après la mise en service du SIS en vertu du présent règlement, établir un rapport sur le fonctionnement technique du SIS central et de l'infrastructure de communication, y compris la sécurité qu'ils offrent, et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires. La Commission devrait procéder à une évaluation globale tous les quatre ans.

(54) Afin de garantir le bon fonctionnement du SIS, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne la détermination des circonstances dans lesquelles des photographies et des images faciales peuvent être utilisées aux fins de l'identification de personnes dans un contexte autre que celui des points de passage frontaliers habituels. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer» ([2]). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(55) Étant donné que les objectifs du présent règlement, à savoir l'établissement d'un système d'information de l'Union et la fixation de règles applicables à ce système ainsi que l'échange d'informations supplémentaires connexes, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent en raison de leur nature l'être mieux au niveau de l'Union, celle-ci 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.

(56) 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, le présent règlement respecte pleinement la protection des données à caractère personnel conformément à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, tout en cherchant à assurer un environnement sûr pour toutes les personnes résidant sur le territoire de l'Union et à protéger les migrants en situation irrégulière contre l'exploitation et la traite des êtres humains. Dans les affaires concernant un enfant, l'intérêt supérieur de l'enfant devrait être une considération primordiale.

(57) Les coûts estimés de la mise à niveau des systèmes nationaux et de la mise en œuvre des nouvelles fonctionnalités envisagées dans le présent règlement sont inférieurs au solde restant dans la ligne budgétaire destinée aux frontières intelligentes prévue dans le règlement (UE) nº 515/2014 du Parlement européen et du Conseil ([3]). En conséquence, il convient d'attribuer aux États membres et à l'eu-LISA un financement pour le développement de systèmes informatiques permettant la gestion des flux migratoires aux frontières extérieures conformément au règlement (UE) nº 515/2014. Il convient d'assurer un suivi des coûts financiers de la mise à niveau du SIS et de la mise en œuvre du présent règlement. Si les coûts estimés sont plus élevés, il convient de mettre à disposition un financement de l'Union pour soutenir les États membres conformément au cadre financier pluriannuel applicable.

(58) Conformément aux articles 1er et 2 du protocole nº 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.

([1]) Règlement (UE) nº 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).

([2]) JO L 123 du 12.5.2016, p. 1.

([3]) 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 et abrogeant la décision nº 574/2007/CE (JO L 150 du 20.5.2014, p. 143).

(59) 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 ([1]); 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.

(60) 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 ([2]); 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.

(61) 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 ([3]), qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE du Conseil ([4]).

(62) En ce qui concerne la Suisse, le présent règlement constitue un développement des dispositions de l'acquis de Schengen au sens 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 ([5]), qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE, lue en liaison avec l'article 3 de la décision 2008/146/CE du Conseil ([6]).

(63) 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 ([7]), qui relèvent du domaine visé à l'article 1er, point G, de la décision 1999/437/CE, lue en liaison avec l'article 3 de la décision 2011/350/UE du Conseil ([8]).

(64) 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 les décisions 2010/365/UE ([9]) et (UE) 2018/934 ([10]) du Conseil.

(65) En ce qui concerne la Croatie, 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 2011 et il doit être lu en combinaison avec la décision (UE) 2017/733 du Conseil ([11]).

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

(67) Le présent règlement apporte une série d'améliorations au SIS qui le rendront plus efficace, renforceront la protection des données et élargiront les droits d'accès. Certaines de ces améliorations n'exigent pas d'avancées techniques complexes, tandis que d'autres nécessitent des évolutions techniques d'une ampleur variable. Afin que les utilisateurs finaux puissent disposer des améliorations du système aussi vite que possible, le présent règlement

---

([1]) 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 (JO L 131 du 1.6.2000, p. 43).

([2]) 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 (JO L 64 du 7.3.2002, p. 20).

([3]) JO L 176 du 10.7.1999, p. 36.

([4]) Décision 1999/437/CE du Conseil du 17 mai 1999 relative à certaines modalités d'application de l'accord conclu par le Conseil de l'Union européenne et la République d'Islande et le Royaume de Norvège sur l'association de ces États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 176 du 10.7.1999, p. 31).

([5]) JO L 53 du 27.2.2008, p. 52.

([6]) Décision 2008/146/CE du Conseil du 28 janvier 2008 relative à la conclusion, au nom de la Communauté européenne, 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 53 du 27.2.2008, p. 1).

([7]) JO L 160 du 18.6.2011, p. 21.

([8]) 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 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).

([9]) Décision 2010/365/UE 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).

([10]) Décision (UE) 2018/934 du Conseil du 25 juin 2018 concernant la mise en application en République de Bulgarie et en Roumanie des dispositions restantes de l'acquis de Schengen relatives au système d'information Schengen (JO L 165 du 2.7.2018, p. 37).

([11]) Décision (UE) 2017/733 du Conseil du 25 avril 2017 sur l'application en République de Croatie des dispositions de l'acquis de Schengen relatives au système d'information Schengen (JO L 108 du 26.4.2017, p. 31).

apporte des modifications au règlement (CE) nº 1987/2006 en plusieurs étapes. Un certain nombre d'améliorations apportées au système devraient s'appliquer immédiatement, dès l'entrée en vigueur du présent règlement, tandis que d'autres devraient s'appliquer un an ou deux ans après son entrée en vigueur. Le présent règlement devrait s'appliquer dans son intégralité dans un délai de trois ans après son entrée en vigueur. Afin d'éviter les retards dans son application, la mise en œuvre progressive du présent règlement devrait être étroitement suivie.

(68) Le règlement (CE) nº 1987/2006 devrait être abrogé avec effet à compter de la date de l'application intégrale du présent règlement.

(69) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001 du Parlement européen et du Conseil ([1]), et a rendu un avis le 3 mai 2017,

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, et d'assurer l'application des 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

Objet

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

2. Le présent règlement prévoit également des dispositions concernant l'architecture technique du SIS, les responsabilités incombant aux États membres et à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (ci-après dénommée «eu-LISA»), le traitement des données, les droits des personnes concernées et la responsabilité.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) «signalement»: un ensemble de données introduites dans le SIS permettant aux autorités compétentes d'identifier une personne en vue de tenir une conduite particulière à son égard;

2) «informations supplémentaires»: les informations ne faisant pas partie des données d'un signalement stockées dans le SIS, mais en rapport avec des signalements dans le SIS, qui doivent être échangées par l'intermédiaire des bureaux SIRENE:

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

   b) à la suite d'une réponse positive afin que la conduite requise puisse être exécutée;

   c) en cas d'impossibilité d'exécuter la conduite requise;

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

   e) en ce qui concerne la compatibilité des signalements et leur ordre de priorité;

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

3) «données complémentaires»: les données stockées dans le SIS en rapport avec des signalements 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 d'une recherche effectuée dans le SIS;

([1]) Règlement (CE) nº 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).

4) «ressortissant de pays tiers»: toute personne qui n'est pas citoyen de l'Union au sens de l'article 20, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, à l'exception des personnes qui sont bénéficiaires, 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, de droits en matière de libre circulation équivalents à ceux des citoyens de l'Union;

5) «données à caractère personnel»: les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

6) «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, l'enregistrement dans un registre, 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;

7) «correspondance»: la succession des étapes suivantes:

   a) une recherche a été effectuée dans le SIS par un utilisateur final;

   b) cette recherche a révélé l'existence d'un signalement introduit dans le SIS par un autre État membre; et

   c) les données relatives au signalement introduit dans le SIS correspondent aux données de la recherche;

8) «réponse positive»: une correspondance qui satisfait aux critères suivants:

   a) elle a été confirmée par:

      i) l'utilisateur final; ou

      ii) l'autorité compétente conformément aux procédures nationales, lorsque la correspondance en question était fondée sur la comparaison de données biométriques;

   et

   b) une conduite complémentaire est demandée;

9) «État membre signalant»: l'État membre qui a introduit le signalement dans le SIS;

10) «État membre d'octroi»: l'État membre qui envisage d'octroyer ou de prolonger un titre de séjour ou un visa de long séjour, ou qui a octroyé ou prolongé un titre de séjour ou un visa de long séjour, et qui participe à la procédure de consultation avec un autre État membre;

11) «État membre d'exécution»: l'État membre qui exécute ou a exécuté la conduite demandée à la suite d'une réponse positive;

12) «utilisateur final»: un membre du personnel d'une autorité compétente autorisé à effectuer des recherches directement dans le CS-SIS, le N.SIS ou dans une copie technique de ceux-ci;

13) «données biométriques»: les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques ou physiologiques d'une personne physique, qui permettent ou confirment son identification unique à savoir les photographies, les images faciales et les données dactyloscopiques;

14) «données dactyloscopiques»: 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;

15) «image faciale»: les images numériques du visage, d'une résolution et d'une qualité d'image suffisantes pour servir à l'établissement automatisé de correspondances biométriques;

16) «retour»: le retour au sens de l'article 3, point 3), de la directive 2008/115/CE;

17) «interdiction d'entrée»: l'interdiction d'entrée au sens de l'article 3, point 6), de la directive 2008/115/CE;

18) «infractions terroristes»: les infractions prévues par le droit national visées aux articles 3 à 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil ([1]) ou qui sont équivalentes à l'une de ces infractions pour les États membres qui ne sont pas liés par cette directive;

19) «titre de séjour»: un titre de séjour au sens de l'article 2, point 16), du règlement (UE) 2016/399 du Parlement européen et du Conseil ([2]);

20) «visa de long séjour»: un visa de long séjour tel qu'il est visé à l'article 18, point 1, de la convention d'application de l'accord de Schengen;

21) «menace pour la santé publique»: une menace pour la santé publique au sens de l'article 2, point 21), du règlement (UE) 2016/399.

([1]) Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

([2]) 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) (JO L 77 du 23.3.2016, p. 1).

Article 4

Architecture technique et mode de fonctionnement du SIS

1. Le SIS se compose:

a) d'un système central (ci-après dénommé «SIS central») comprenant:

   i) une fonction de support technique (ci-après dénommée «CS-CIS») contenant une base de données (ci-après dénommée «base de données du SIS»), et comprenant un CS-SIS de secours;

   ii) une interface nationale uniforme (ci-après dénommée «NI-SIS»);

b) d'un système national (ci-après dénommé «N.SIS») dans chaque État membre, constitué des systèmes de données nationaux reliés au SIS central, y compris au moins un N.SIS de secours national ou partagé; et

c) d'une infrastructure de communication entre le CS-SIS, le CS-SIS de secours et le NI-SIS de secours (ci-après dénommée «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.

Un N.SIS, tel que visé au point b), peut contenir un fichier de données (ci-après dénommé «copie nationale») comportant une copie complète ou partielle de la base de données du SIS. Deux États membres ou plus peuvent mettre en place dans l'un de leurs N.SIS une copie partagée qui peut être utilisée conjointement par ces États membres. Cette copie partagée est considérée comme la copie nationale de chacun de ces États membres.

Un N.SIS de secours partagé, tel que visé au point b), peut être utilisé conjointement par deux États membres ou plus. Dans de tels cas, le N.SIS de secours partagé est considéré comme le N.SIS de secours de chacun de ces États membres. Le N.SIS et le N.SIS de secours peuvent être utilisés simultanément en vue d'assurer la disponibilité continue pour les utilisateurs finaux.

Les États membres souhaitant mettre en place une copie partagée ou un N.SIS de secours partagé à utiliser conjointement conviennent par écrit de leurs responsabilités respectives. Ils notifient leur arrangement à la Commission.

L'infrastructure de communication apporte son soutien et sa contribution pour assurer la disponibilité continue du SIS. Elle comprend des chemins redondants et séparés pour les connexions entre le CS-SIS et le CS-SIS de secours, ainsi que des chemins redondants et séparés pour les connexions entre chaque point d'accès national du réseau au SIS et le CS-SIS et le CS-SIS de secours.

2. Les États membres introduisent, mettent à jour, et suppriment les données du SIS et effectuent des recherches dans les données du SIS par l'intermédiaire de leur propre N.SIS. Les États membres utilisant une copie nationale partielle ou complète ou une copie partagée partielle ou complète mettent cette copie à disposition pour effectuer des recherches automatisées sur le territoire de chacun de ces États membres. La copie nationale partielle ou la copie partagée partielle contient au moins les données énumérées à l'article 20, paragraphe 2, points a) à v). Il n'est pas possible d'effectuer des recherches dans les fichiers de données des N.SIS des autres États membres, sauf s'il s'agit de copies partagées.

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 ce système. Le CS-SIS et le CS-SIS de secours sont situés sur les deux sites techniques de l'eu-LISA.

4. L'eu-LISA met en œuvre des solutions techniques pour renforcer la disponibilité continue du SIS, soit par le fonctionnement simultané du CS-SIS et du CS-SIS de secours, pour autant que le CS-SIS de secours demeure capable d'assurer le fonctionnement du SIS en cas de défaillance du CS-SIS, soit par la duplication du système ou de ses éléments. Nonobstant les exigences de procédure fixées à l'article 10 du règlement (UE) 2018/1726, l'eu-LISA réalise, au plus tard le 28 décembre 2019, une étude sur les options de solutions techniques, comportant une analyse d'impact indépendante et une analyse coûts/avantages.

5. Si nécessaire dans des circonstances exceptionnelles, l'eu-LISA peut provisoirement mettre en place une copie supplémentaire de la base de données du SIS.

6. Le CS-SIS assure les services nécessaires à l'introduction et au traitement des données du SIS, y compris les recherches dans la base de données du SIS. Pour les États membres qui utilisent une copie nationale ou partagée, le CS-SIS assure:

a) les mises à jour en ligne des copies nationales;

b) la synchronisation et la cohérence entre les copies nationales et la base de données du SIS; et

c) les opérations d'initialisation et de restauration des copies nationales.

7. Le CS-SIS assure une 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. 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 6.

2. Des fonds sont alloués à partir de l'enveloppe de 791 000 000 EUR prévue à l'article 5, paragraphe 5, point b), du règlement (UE) nº 515/2014 pour couvrir les coûts de mise en œuvre du présent règlement.

3. Il est alloué à l'eu-LISA un montant de 31 098 000 EUR à partir de l'enveloppe visée au paragraphe 2, sans préjuger d'autres financements à cette fin à partir d'autres sources du budget général de l'Union. Ce financement est mis en œuvre dans le cadre d'une gestion indirecte et contribue à la réalisation des évolutions techniques requises au titre du présent règlement en ce qui concerne le SIS central et l'infrastructure de communication ainsi que les activités de formation y afférentes.

4. Les États membres participant au règlement (UE) nº 515/2014 reçoivent, à partir de l'enveloppe visée au paragraphe 2, une dotation supplémentaire globale de 36 810 000 EUR à distribuer à parts égales sous la forme de montant forfaitaire s'ajoutant à leur dotation de base. Ce financement est mis en œuvre dans le cadre d'une gestion partagée et il est entièrement destiné à la mise à niveau rapide et efficace des systèmes nationaux concernés conformément aux exigences du présent règlement.

5. 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 assume la responsabilité de garantir aux utilisateurs finaux une disponibilité continue des données du SIS.

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

Article 7

Office N.SIS et bureau SIRENE

1. Chaque État membre désigne une autorité (ci-après dénommée «office N.SIS») qui assume la responsabilité centrale de son 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 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.

2. Chaque État membre désigne une autorité nationale qui est pleinement opérationnelle 24 heures sur 24 et 7 jours sur 7 et qui assure l'échange et la disponibilité de toutes les informations supplémentaires (ci-après dénommée «bureau SIRENE»), conformément au manuel SIRENE. Chaque bureau SIRENE sert de point de contact unique pour son État membre pour l'échange des informations supplémentaires concernant les signalements et pour faciliter les conduites à tenir demandées lorsque des signalements concernant des personnes ont été introduits dans le SIS et que ces personnes sont localisées à la suite d'une réponse positive.

Chaque bureau SIRENE dispose, dans le respect du droit national, d'un accès facile direct ou indirect à toutes les informations nationales pertinentes, y compris aux bases de données nationales et à toutes les informations sur les signalements de son État membre, ainsi qu'aux avis d'experts, afin d'être à même de réagir aux demandes d'informations supplémentaires rapidement et dans les délais prévus à l'article 8.

Les bureaux SIRENE coordonnent 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'eu-LISA les coordonnées de leur office N.SIS et de leur bureau SIRENE. L'eu-LISA publie la liste des offices N.SIS et des bureaux SIRENE ainsi que la liste visée à l'article 41, paragraphe 8.

Article 8

Échange d'informations supplémentaires

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

2. Les informations supplémentaires ne sont utilisées qu'aux fins auxquelles elles ont été transmises conformément à l'article 49, à moins que l'État membre signalant n'ait consenti au préalable à une autre utilisation.

3. Les bureaux SIRENE s'acquittent de leurs tâches de manière rapide et efficace, notamment en répondant aux demandes d'informations supplémentaires dans les meilleurs délais, mais au plus tard 12 heures après la réception de la demande.

Les formulaires SIRENE concernant des demandes d'informations supplémentaires présentant la priorité la plus élevée portent la mention «URGENT» et les motifs de l'urgence sont précisés.

4. La Commission adopte des actes d'exécution pour établir les modalités relatives aux tâches confiées aux bureaux SIRENE en vertu du présent règlement et à l'échange d'informations supplémentaires sous la forme d'un manuel intitulé «manuel SIRENE». Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 9

Conformité technique et fonctionnelle

1. Pour permettre une transmission rapide et efficace des données, chaque État membre respecte, 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 SIS central.

2. Si un État membre utilise une copie nationale, il veille, au moyen des services fournis par le CS-SIS et des mises à jour automatiques visées à l'article 4, paragraphe 6, à ce que les données stockées dans la copie nationale soient identiques à la base de données du SIS et compatibles avec elle, et à ce qu'une recherche dans cette copie nationale produise un résultat équivalent à celui d'une recherche dans la base de données du SIS.

3. Les utilisateurs finaux reçoivent les données dont ils ont besoin pour s'acquitter de leurs tâches, en particulier, et si nécessaire, toutes les données disponibles permettant d'identifier la personne concernée et d'exécuter la conduite à tenir demandée.

4. Les États membre et l'eu-LISA réalisent régulièrement des tests pour vérifier la conformité technique des copies nationales visées au paragraphe 2. Les résultats de ces tests sont pris en considération dans le cadre du mécanisme instauré par le règlement (UE) nº 1053/2013 du Conseil ([1]).

5. La Commission adopte des actes d'exécution pour établir et préciser les normes communes, les protocoles et les procédures techniques visés au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

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, nécessaires pour:

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

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

c) empêcher toute lecture, copie ou modification ou tout retrait non autorisés de supports de données (contrôle des supports de données);

([1]) Règlement (UE) nº 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).

d) empêcher l'introduction non autorisée de données ainsi que le contrôle, la modification ou la suppression non autorisés de données à caractère personnel stockées (contrôle du stockage);

e) empêcher l'utilisation des systèmes de traitement automatisé de données par des personnes non autorisées au moyen de matériel de transmission de données (contrôle des utilisateurs);

f) empêcher le traitement non autorisé de données dans le SIS et toute modification ou tout effacement non autorisés de données traitées dans le SIS (contrôle de la saisie des données);

g) garantir que les personnes autorisées à utiliser un système de traitement automatisé de données ne puissent avoir accès qu'aux données couvertes par leur autorisation d'accès, uniquement grâce à des identifiants d'utilisateur individuels et uniques et à des modes d'accès confidentiels (contrôle de l'accès aux données);

h) s'assurer que toutes les autorités ayant un droit d'accès au SIS ou aux installations de traitement de données créent des profils décrivant les fonctions et responsabilités des personnes autorisées à avoir accès aux données, à les introduire, à les mettre à jour, et à les supprimer et à effectuer des recherches dans ces données et mettent sans tarder, et à leur demande, ces profils à la disposition des autorités de contrôle visées à l'article 55, paragraphe 1 (profils des membres du personnel);

i) garantir la possibilité de vérifier et d'établir à quels organismes des données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données (contrôle de la transmission);

j) garantir la possibilité de vérifier et d'établir 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);

k) empêcher toute lecture, copie, modification ou suppression non autorisées de données à caractère personnel pendant la transmission de données à caractère personnel ou durant le transport de supports de données, en particulier au moyen de techniques de cryptage adaptées (contrôle du transport);

l) contrôler l'efficacité des mesures de sécurité prévues au présent paragraphe et prendre les mesures organisationnelles nécessaires en matière de contrôle interne pour assurer le respect du présent règlement (autocontrôle);

m) garantir le rétablissement des systèmes installés en cas d'interruption (rétablissement); et

n) garantir que le SIS exécute correctement ses fonctions, que les erreurs soient signalées (fiabilité) et que les données à caractère personnel stockées dans le SIS ne puissent pas être corrompues par le dysfonctionnement du système (intégrité).

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

3. Les États membres prennent des mesures équivalentes à celles visées au paragraphe 1 du présent article pour assurer la sécurité du traitement des données du SIS effectué par les autorités visées à l'article 34.

4. Les mesures décrites aux paragraphes 1, 2 et 3 peuvent faire partie d'une approche et d'un plan de sécurité génériques au niveau national englobant des systèmes informatiques multiples. Dans de tels cas, les exigences énoncées au présent article et leur applicabilité au SIS sont clairement identifiables dans ce plan et respectées par ce plan.

Article 11

Confidentialité — États membres

1. 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 en matière de secret professionnel ou leur impose des obligations de confidentialité équivalentes, conformément à son droit national. 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.

2. Lorsqu'un État membre coopère avec des prestataires externes sur toute tâche liée au SIS, il suit de près les activités des prestataires afin de veiller au respect de l'ensemble des dispositions du présent règlement, notamment en ce qui concerne la sécurité, la confidentialité et la protection des données.

3. La gestion opérationnelle des N.SIS ou de copies techniques n'est en aucun cas confiée à une entreprise ou organisation privée.

Article 12

Tenue de registres au niveau national

1. Les États membres veillent à ce que tous les accès à des données à caractère personnel et tous les échanges de données à caractère personnel au sein du CS-SIS soient enregistrés dans leur N.SIS afin de pouvoir contrôler la licéité de la recherche et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS et de garantir l'intégrité et la sécurité des données. Cette exigence ne s'applique pas aux processus automatiques visés à l'article 4, paragraphe 6, points a), b) et c).

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

3. Par dérogation au paragraphe 2 du présent article, si la recherche est effectuée à l'aide de données dactyloscopiques ou d'une image faciale conformément à l'article 33, les registres indiquent le type de données utilisées pour effectuer la recherche au lieu des données réelles.

4. Les registres ne sont utilisés qu'aux fins visées au paragraphe 1 et sont supprimés trois ans après leur création. Les registres contenant l'historique des signalements sont supprimés trois ans après la suppression des signalements.

5. Les registres peuvent être conservés au-delà des périodes visées au paragraphe 4 s'ils sont nécessaires à des procédures de contrôle déjà engagées.

6. Les autorités nationales compétentes chargées de contrôler la licéité des recherches et la licéité des traitements de données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS, et de garantir l'intégrité et la sécurité des données, ont accès aux registres, dans les limites de leurs compétences et sur demande, 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.

Article 14

Formation du personnel

1. 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 la sécurité des données, sur les droits fondamentaux, dont les règles en matière de protection des données, et sur les règles et procédures relatives au traitement des données énoncées dans le manuel SIRENE. Le personnel est informé de toute disposition pertinente relative aux infractions pénales et aux sanctions, dont celles prévues à l'article 59.

2. Les États membres disposent d'un programme de formation SIS national qui comporte une formation pour les utilisateurs finaux ainsi que pour le personnel des bureaux SIRENE.

Ce programme de formation peut faire partie d'un programme de formation général au niveau national englobant des formations dans d'autres domaines pertinents.

3. Des formations communes sont organisées au niveau de l'Union au moins une fois par an pour renforcer la coopération entre les bureaux SIRENE.

CHAPITRE III

RESPONSABILITÉS DE L'eu-LISA

Article 15

Gestion opérationnelle

1. L'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 utilise en permanence la meilleure technologie disponible, sous réserve d'une analyse coûts/avantages.

2. Il incombe également à l'eu-LISA d'assumer les tâches ci-après en ce qui concerne l'infrastructure de communication:

a) la supervision;

b) la sécurité;

c) la coordination des relations entre les États membres et le fournisseur;

d) les tâches relatives à l'exécution du budget;

e) l'acquisition et le renouvellement; et

f) les questions contractuelles.

3. L'eu-LISA est également chargée des tâches ci-après en ce qui concerne les bureaux SIRENE et la communication entre les bureaux SIRENE:

a) la coordination, la gestion et le soutien des activités de test;

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; et

c) la gestion des effets des modifications techniques lorsqu'elles ont une incidence à la fois sur le SIS et sur les échanges d'informations supplémentaires entre les bureaux SIRENE.

4. L'eu-LISA élabore et gère un dispositif et des procédures de contrôle de qualité des données du CS-SIS. Elle présente, à intervalles réguliers, des rapports aux États membres à cet effet.

L'eu-LISA présente à la Commission, à intervalles réguliers, un rapport indiquant les problèmes rencontrés et les États membres concernés.

La Commission présente au Parlement européen et au Conseil, à intervalles réguliers, un rapport sur les problèmes rencontrés quant à la qualité des données.

5. L'eu-LISA s'acquitte également des tâches liées à l'offre d'une formation relative à l'utilisation technique du SIS et aux mesures destinées à améliorer la qualité des données du SIS.

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. Ces tâches incluent également la coordination, la gestion et le soutien des activités de test concernant le SIS central et les N.SIS qui garantissent que le SIS central et les N.SIS fonctionnent conformément aux exigences de conformité technique et fonctionnelle énoncées à l'article 9.

7. La Commission adopte des actes d'exécution pour établir les exigences techniques de l'infrastructure de communication. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 16

Sécurité — eu-LISA

1. L'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, nécessaires pour:

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

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

c) empêcher toute lecture, copie ou modification ou tout retrait non autorisés de supports de données (contrôle des supports de données);

d) empêcher l'introduction non autorisée de données ainsi que le contrôle, la modification ou la suppression non autorisés de données à caractère personnel stockées (contrôle du stockage);

e) empêcher l'utilisation des systèmes de traitement automatisé de données par des personnes non autorisées au moyen de matériel de transmission de données (contrôle des utilisateurs);

f) empêcher le traitement non autorisé de données dans le SIS et toute modification ou tout effacement non autorisés de données traitées dans le SIS (contrôle de la saisie des données);

g) garantir que les personnes autorisées à utiliser un système de traitement automatisé de données ne puissent avoir accès qu'aux données couvertes par leur autorisation d'accès, uniquement grâce à des identifiants d'utilisateur individuels et uniques et à des modes d'accès confidentiels (contrôle de l'accès aux données);

h) créer des profils décrivant les fonctions et responsabilités des personnes autorisées à avoir accès aux données ou aux installations de traitement de données, et mettre ces profils à la disposition du Contrôleur européen de la protection des données, sans tarder et à la demande de celui-ci (profils des membres du personnel);

i) garantir la possibilité de vérifier et d'établir à quels organismes des données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données (contrôle de la transmission);

j) garantir la possibilité de vérifier et d'établir 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);

k) empêcher toute lecture, copie, modification ou suppression non autorisées de données à caractère personnel pendant la transmission de données à caractère personnel ou durant le transport de supports de données, en particulier au moyen de techniques de cryptage adaptées (contrôle du transport);

l) contrôler l'efficacité des mesures de sécurité visées au présent paragraphe et prendre les mesures organisationnelles nécessaires en matière de contrôle interne pour assurer le respect du présent règlement (autocontrôle);

m) garantir le rétablissement des systèmes installés en cas d'interruption des opérations (rétablissement);

n) garantir que le SIS exécute correctement ses fonctions, que les erreurs soient signalées (fiabilité) et que les données à caractère personnel conservées dans le SIS ne puissent pas être corrompues par le dysfonctionnement du système (intégrité); et

o) garantir la sécurité de ses sites techniques.

2. L'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 l'intermédiaire de l'infrastructure de communication.

Article 17

Confidentialité — eu-LISA

1. Sans préjudice de l'article 17 du statut, l'eu-LISA applique à l'égard de tous les membres de son personnel appelés à travailler avec des données du SIS des règles appropriées en matière de secret professionnel ou leur impose des obligations de confidentialité équivalentes d'un niveau comparable à celui prévu 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'eu-LISA prend des mesures équivalentes à celles visées au paragraphe 1 pour assurer la confidentialité de l'échange d'informations supplémentaires par l'intermédiaire de l'infrastructure de communication.

3. Lorsque l'eu-LISA coopère avec des prestataires externes sur toute tâche liée au SIS, elle suit de près les activités des prestataires afin de veiller au respect de l'ensemble des dispositions du présent règlement, notamment en ce qui concerne la sécurité, la confidentialité et la protection des données.

4. La gestion opérationnelle du CS-SIS n'est en aucun cas confiée à une entreprise ou organisation privée.

Article 18

Tenue de registres au niveau central

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

2. Les registres indiquent, en particulier, l'historique du signalement, la date et l'heure de l'opération de traitement des données, les données utilisées pour effectuer une recherche, la référence aux données traitées et les identifiants d'utilisateur individuels et uniques de l'autorité compétente traitant les données.

3. Par dérogation au paragraphe 2 du présent article, si la recherche est effectuée à l'aide de données dactyloscopiques ou d'images faciales conformément à l'article 33, les registres indiquent le type de données utilisées pour effectuer la recherche au lieu des données réelles.

4. Les registres ne sont utilisés qu'aux fins visées au paragraphe 1, et sont supprimés trois ans après leur création. Les registres contenant l'historique des signalements sont supprimés trois ans après la suppression des signalements.

5. Les registres peuvent être conservés au-delà des périodes visées au paragraphe 4 s'ils sont nécessaires à des procédures de contrôle déjà engagées.

6. À des fins d'autocontrôle et pour garantir le bon fonctionnement du CS-SIS ainsi que l'intégrité et la sécurité des données, l'eu-LISA a accès à ces registres, dans les limites de ses compétences.

Le Contrôleur européen de la protection des données a accès à ces registres à sa demande, dans les limites de ses compétences et afin de pouvoir s'acquitter de ses tâches.

CHAPITRE IV

INFORMATION DU PUBLIC

Article 19

Campagnes d'information sur le SIS

Au début de l'application du présent règlement, la Commission, en coopération avec les autorités de contrôle et le Contrôleur européen de la protection des données, organise une campagne visant à faire connaître au public les objectifs du SIS, les données stockées dans le SIS, les autorités ayant accès au SIS et les droits des personnes concernées. La Commission mène régulièrement des campagnes de ce type, en coopération avec les autorités de contrôle et le Contrôleur européen de la protection des données. La Commission gère un site internet accessible au public qui fournit toutes les informations pertinentes relatives au SIS. Les États membres, en coopération avec leurs autorités de contrôle, élaborent et mettent en œuvre les politiques nécessaires pour assurer l'information générale de leurs citoyens et résidents sur le SIS.

CHAPITRE V

SIGNALEMENTS DE RESSORTISSANTS DE PAYS TIERS AUX FINS DE NON-ADMISSION ET D'INTERDICTION DE SÉJOUR

Article 20

Catégories de données

1. Sans préjudice de l'article 8, paragraphe 1, ou des dispositions du présent règlement prévoyant le stockage de données complémentaires, le SIS ne comporte que les catégories de données qui sont fournies par chaque État membre nécessaires aux fins prévues aux articles 24 et 25.

2. Tout signalement dans le SIS qui comporte des renseignements concernant des personnes comprend uniquement les données suivantes:

a) les noms;

b) les prénoms;

c) les noms 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 genre;

i) toutes les nationalités possédées;

j) l'indication que la personne concernée:

   i) est armée;

   ii) est violente;

   iii) s'est enfuie ou échappée;

   iv) présente un risque de suicide;

   v) représente une menace pour la santé publique; ou

   vi) est impliquée dans une activité visée aux articles 3 à 14 de la directive (UE) 2017/541;

k) le motif du signalement;

l) l'autorité qui a créé le signalement;

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

n) la conduite à tenir en cas de réponse positive;

o) les liens vers d'autres signalements en vertu de l'article 48;

p) l'indication que la personne concernée est ou non un membre de la famille d'un citoyen de l'Union ou une autre personne qui est bénéficiaire du droit à la libre circulation visé à l'article 26;

q) l'indication que la décision de non-admission et d'interdiction de séjour est ou non fondée sur:

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

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

iii) le contournement du droit national ou de l'Union relatif à l'entrée et au séjour visé à l'article 24, paragraphe 2, point c);

iv) une interdiction d'entrée visée à l'article 24, paragraphe 1, point b); ou

v) une mesure restrictive visée à l'article 25;

r) le type d'infraction;

s) la catégorie des documents d'identification de la personne;

t) le pays de délivrance des documents d'identification de la personne;

u) le ou les numéros des documents d'identification de la personne;

v) la date de délivrance des documents d'identification de la personne;

w) les photographies et les images faciales;

x) les données dactyloscopiques;

y) une copie des documents d'identification, si possible en couleurs.

3. La Commission adopte des actes d'exécution pour établir et préciser les règles techniques nécessaires pour l'introduction, la mise à jour, et la suppression des données visées au paragraphe 2 du présent article et pour les recherches dans ces données, ainsi que les normes communes visées au paragraphe 4 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

4. Ces règles techniques sont similaires pour les recherches dans le CS-SIS, dans les copies nationales ou partagées et dans les copies techniques réalisées en vertu de l'article 41, paragraphe 2. Elles sont fondées sur des normes communes.

Article 21

Proportionnalité

1. Avant d'introduire un signalement et de prolonger la durée de validité d'un signalement, les États membres vérifient si le cas est suffisamment approprié, pertinent et important pour justifier un signalement dans le SIS.

2. Lorsque la décision de non-admission et d'interdiction de séjour visée à l'article 24, paragraphe 1, point a), est liée à une infraction terroriste, le cas est considéré comme étant suffisamment approprié, pertinent et important pour justifier un signalement dans le SIS. Pour des raisons de sécurité publique ou nationale, les États membres peuvent, à titre exceptionnel, s'abstenir d'introduire le signalement si celui-ci risque de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires.

Article 22

Exigence à remplir pour l'introduction d'un signalement

1. Tout signalement introduit dans le SIS comprend au minimum l'ensemble des données visées à l'article 20, paragraphe 2, points a), g), k), m), n), et q). Les autres données visées audit paragraphe sont également introduites dans le SIS, si elles sont disponibles.

2. Les données visées à l'article 20, paragraphe 2, point e), du présent règlement ne sont introduites que si cela est strictement nécessaire aux fins de l'identification du ressortissant de pays tiers concerné. Lors de l'introduction de ces données, les États membres veillent au respect de l'article 9 du règlement (UE) 2016/679.

Article 23

Compatibilité des signalements

1. Avant d'introduire un signalement, l'État membre vérifie si la personne concernée fait déjà l'objet d'un signalement dans le SIS. À cette fin, il est procédé à une vérification à l'aide des données dactyloscopiques, si ces données sont disponibles.

2. Chaque État membre n'introduit dans le SIS qu'un seul signalement par personne. Si nécessaire, de nouveaux signalements concernant la même personne peuvent être introduits par d'autres États membres, conformément au paragraphe 3.

3. Lorsqu'une personne fait déjà l'objet d'un signalement dans le SIS, l'État membre qui souhaite introduire un nouveau signalement vérifie qu'il n'y a pas d'incompatibilité entre les signalements. S'il n'y a pas d'incompatibilité, l'État membre peut introduire le nouveau signalement. Si les signalements sont incompatibles, les bureaux SIRENE des États membres concernés se consultent par la voie d'échanges d'informations supplémentaires pour parvenir à un accord. Les règles relatives à la compatibilité des signalements sont fixées dans le manuel SIRENE. Il peut être dérogé aux règles de compatibilité après consultation entre les États membres si des intérêts nationaux essentiels sont en jeu.

4. En cas de réponses positives à des signalements multiples concernant la même personne, l'État membre d'exécution observe les règles de priorité pour les signalements fixées dans le manuel SIRENE.

Si une personne fait l'objet de signalements multiples introduits par différents États membres, les signalements en vue d'une arrestation introduits conformément à l'article 26 du règlement (UE) 2018/1862 sont exécutés en priorité, sous réserve de l'article 25 dudit règlement.

Article 24

Conditions d'introduction des signalements aux fins de non-admission et d'interdiction de séjour

1. Les États membres introduisent un signalement aux fins de non-admission et d'interdiction de séjour lorsque l'une des conditions ci-après est remplie:

a) l'État membre a conclu, sur la base d'une évaluation individuelle comprenant une appréciation de la situation personnelle du ressortissant de pays tiers concerné et des conséquences du refus d'entrée et de séjour, que la présence de ce ressortissant de pays tiers sur son territoire représente une menace pour l'ordre public, la sécurité publique ou la sécurité nationale et l'État membre a, par conséquent, adopté une décision judiciaire ou administrative de non-admission et d'interdiction de séjour conformément à son droit national et émis un signalement national aux fins de non-admission et d'interdiction de séjour; ou

b) l'État membre a émis une interdiction d'entrée conformément à des procédures respectant la directive 2008/115/CE au sujet d'un ressortissant de pays tiers.

2. Les situations couvertes par le paragraphe 1, point a), se produisent lorsque:

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

b) il existe des raisons sérieuses de croire qu'un ressortissant de pays tiers a commis une infraction pénale grave, y compris une infraction terroriste, ou il existe des indications claires de son intention de commettre une telle infraction sur le territoire d'un État membre; ou

c) un ressortissant de pays tiers a contourné ou tenté de contourner le droit national ou de l'Union relatif à l'entrée et au séjour sur le territoire des États membres.

3. L'État membre signalant veille à ce que le signalement prenne effet dans le SIS dès que le ressortissant de pays tiers concerné a quitté le territoire des États membres ou dès que possible lorsque l'État membre signalant a obtenu des indications claires que le ressortissant de pays tiers a quitté le territoire des États membres, afin d'empêcher ce ressortissant de pays tiers d'y entrer à nouveau.

4. Les personnes à l'égard desquelles une décision de non-admission et d'interdiction de séjour est prise conformément au paragraphe 1 disposent d'un droit de recours. Ces recours sont exercés conformément au droit national et de l'Union, qui prévoient un recours effectif à introduire devant une juridiction.

Article 25

Conditions d'introduction des signalements concernant les ressortissants de pays tiers qui font l'objet de mesures restrictives

1. Les signalements concernant les ressortissants de pays tiers qui font l'objet d'une mesure restrictive visant à les empêcher d'entrer sur le territoire des États membres ou de transiter par ce territoire, prise conformément à des actes juridiques adoptés par le Conseil, y compris les mesures mettant en œuvre une interdiction de voyager imposée par le Conseil de sécurité des Nations unies, font, dans la mesure où il est satisfait aux exigences en matière de qualité des données, l'objet d'une introduction dans le SIS aux fins de non-admission et d'interdiction de séjour.

2. Les signalements sont introduits, mis à jour et supprimés par l'autorité compétente de l'État membre qui exerce la présidence du Conseil de l'Union européenne au moment de l'adoption de la mesure. Si cet État membre n'a pas accès au SIS ou aux signalements introduits conformément au présent règlement, la responsabilité est assumée par l'État membre qui exerce la présidence suivante et qui a accès au SIS, y compris aux signalements introduits conformément au présent règlement.

Les États membres mettent en place les procédures nécessaires pour introduire, mettre à jour et supprimer ces signalements.

Article 26

Conditions d'introduction des signalements concernant les ressortissants de pays tiers qui sont bénéficiaires du droit à la libre circulation dans l'Union

1. Un signalement concernant un ressortissant de pays tiers qui est bénéficiaire du droit à la libre circulation dans l'Union conformément à la directive 2004/38/CE ou conformément à un accord conclu entre, d'une part, l'Union ou l'Union et ses États membres et, d'autre part, un pays tiers, doit être conforme aux règles adoptées pour la mise en œuvre de ladite directive ou dudit accord.

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

Article 27

Consultation préalable à l'octroi ou à la prolongation d'un titre de séjour ou d'un visa de long séjour

Lorsqu'un État membre envisage d'octroyer ou de prolonger un titre de séjour ou un visa de long séjour au bénéfice d'un ressortissant de pays tiers faisant l'objet d'un signalement aux fins de non-admission et d'interdiction de séjour introduit par un autre État membre, les États membres concernés se consultent, par la voie d'échange d'informations supplémentaires, conformément aux règles suivantes:

a) l'État membre d'octroi consulte l'État membre signalant avant d'octroyer ou de prolonger le titre de séjour ou le visa de long séjour;

b) l'État membre signalant répond à la demande de consultation dans un délai de dix jours civils;

c) l'absence de réponse dans le délai visé au point b) équivaut à une absence d'objection de la part de l'État membre signalant quant à l'octroi ou la prolongation du titre de séjour ou du visa de long séjour;

d) lorsqu'il prend la décision en question, l'État membre d'octroi tient compte des motifs de la décision de l'État membre signalant et prend en considération, conformément au droit national, toute menace pour l'ordre public ou la sécurité publique que peut représenter la présence du ressortissant de pays tiers en question sur le territoire des États membres;

e) l'État membre d'octroi notifie sa décision à l'État membre signalant; et

f) lorsque l'État membre d'octroi notifie à l'État membre signalant son intention d'octroyer ou de prolonger le titre de séjour ou le visa de long séjour, ou sa décision de le faire, l'État membre signalant supprime le signalement aux fins de non-admission et d'interdiction de séjour.

La décision finale d'octroyer ou non un titre de séjour ou un visa de long séjour à un ressortissant de pays tiers incombe à l'État membre d'octroi.

Article 28

Consultation préalable à l'introduction d'un signalement aux fins de non-admission et d'interdiction de séjour

Lorsqu'un État membre a pris une décision visée à l'article 24, paragraphe 1, et envisage d'introduire un signalement aux fins de non-admission et d'interdiction de séjour concernant un ressortissant de pays tiers qui est titulaire d'un titre de séjour ou d'un visa de long séjour en cours de validité octroyé par un autre État membre, les États membres concernés se consultent, par la voie d'échange d'informations supplémentaires, conformément aux règles suivantes:

a) l'État membre qui a pris la décision visée à l'article 24, paragraphe 1, informe l'État membre d'octroi de sa décision;

b) les informations échangées en vertu du point a) du présent article contiennent suffisamment de précisions quant aux motifs de la décision visée à l'article 24, paragraphe 1;

c) sur la base des informations fournies par l'État membre qui a pris la décision visée à l'article 24, paragraphe 1, l'État membre d'octroi examine s'il existe des motifs de retirer le titre de séjour ou le visa de long séjour;

d) lorsqu'il prend la décision en question, l'État membre d'octroi tient compte des motifs de la décision de l'État membre qui a pris la décision visée à l'article 24, paragraphe 1, et il prend en considération, conformément au droit national, toute menace pour l'ordre public ou la sécurité publique que pourrait représenter la présence du ressortissant de pays tiers en question sur le territoire des États membres;

e) dans un délai de 14 jours civils à compter de la réception de la demande de consultation, l'État membre d'octroi notifie sa décision à l'État membre qui a pris la décision visée à l'article 24, paragraphe 1, ou, si l'État membre d'octroi n'a pas pu prendre de décision dans ce délai, lui adresse une demande motivée de prolongation exceptionnelle du délai de réponse de maximum 12 jours civils supplémentaires;

f) lorsque l'État membre d'octroi informe l'État membre qui a pris la décision visée à l'article 24, paragraphe 1, qu'il maintient le titre de séjour ou le visa de long séjour, l'État membre qui a pris la décision n'introduit pas de signalement aux fins de non-admission et d'interdiction de séjour.

Article 29

Consultation a posteriori après l'introduction d'un signalement aux fins de non-admission et d'interdiction de séjour

Lorsqu'il apparaît qu'un État membre a introduit un signalement aux fins de non-admission et d'interdiction de séjour concernant un ressortissant de pays tiers qui est titulaire d'un titre de séjour ou d'un visa de long séjour en cours de validité octroyé par un autre État membre, les États membres concernés se consultent, par la voie d'échange d'informations supplémentaires, conformément aux règles suivantes:

a) l'État membre signalant informe l'État membre d'octroi du signalement aux fins de non-admission et d'interdiction de séjour;

b) les informations échangées en vertu du point a) contiennent suffisamment de précisions quant aux motifs du signalement aux fins de non-admission et d'interdiction de séjour;

c) sur la base des informations fournies par l'État membre signalant, l'État membre d'octroi examine s'il existe des motifs de retirer le titre de séjour ou le visa de long séjour;

d) lorsqu'il prend sa décision, l'État membre d'octroi tient compte des motifs de la décision de l'État membre signalant et prend en considération, conformément au droit national, toute menace pour l'ordre public ou la sécurité publique que peut représenter la présence du ressortissant de pays tiers en question sur le territoire des États membres;

e) dans un délai de 14 jours civils à compter de la réception de la demande de consultation, l'État membre d'octroi notifie sa décision à l'État membre signalant ou, si l'État membre d'octroi n'a pas pu prendre de décision dans ce délai, lui adresse une demande motivée de prolongation exceptionnelle du délai de réponse de maximum 12 jours civils supplémentaires;

f) lorsque l'État membre d'octroi informe l'État membre signalant qu'il maintient le titre de séjour ou le visa de long séjour, l'État membre signalant supprime immédiatement le signalement aux fins de non-admission et d'interdiction de séjour.

Article 30

Consultation en cas de réponse positive concernant un ressortissant de pays tiers titulaire d'un titre de séjour ou d'un visa de long séjour en cours de validité

Lorsqu'un État membre obtient une réponse positive à un signalement aux fins de non-admission et d'interdiction de séjour introduit par un État membre concernant un ressortissant de pays tiers qui est titulaire d'un titre de séjour ou d'un visa de long séjour en cours de validité octroyé par un autre État membre, les États membres concernés se consultent par la voie d'échange d'informations supplémentaires, conformément aux règles suivantes:

a) l'État membre d'exécution informe l'État membre signalant de la situation;

b) l'État membre signalant engage la procédure prévue à l'article 29;

c) l'État membre signalant notifie à l'État membre d'exécution le résultat de la consultation.

La décision relative à l'entrée du ressortissant de pays tiers est prise par l'État membre d'exécution conformément règlement (UE) 2016/399.

Article 31

Statistiques sur les échanges d'informations

Les États membres communiquent annuellement à l'eu-LISA des statistiques sur les échanges d'informations ayant eu lieu conformément aux articles 27 à 30, ainsi que sur les cas dans lesquels les délais prévus dans ces articles n'ont pas été respectés.

CHAPITRE VI

RECHERCHE À L'AIDE DE DONNÉES BIOMÉTRIQUES

Article 32

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

1. Seules les photographies, les images faciales et les données dactyloscopiques visées à l'article 20, paragraphe 2, points w) et x), qui répondent à des normes minimales en matière de qualité des données et à des spécifications techniques sont introduites dans le SIS. Avant l'introduction de telles données, il est procédé à un contrôle de qualité visant à établir si les normes minimales en matière de qualité des données et les spécifications techniques ont été respectées.

2. Les données dactyloscopiques introduites dans le SIS peuvent consister en une à dix empreintes digitales à plat et une à dix empreintes digitales roulées. Elles peuvent également comprendre jusqu'à deux empreintes palmaires.

3. Des normes minimales en matière de qualité des données et des spécifications techniques sont établies conformément au paragraphe 4 du présent article pour la conservation des données biométriques visées au paragraphe 1 du présent article. Ces normes minimales en matière de qualité des données et ces spécifications techniques fixent le niveau de qualité requis pour l'utilisation des données aux fins de la vérification de l'identité d'une personne conformément à l'article 33, paragraphe 1, ainsi que pour l'utilisation des données aux fins de l'identification d'une personne conformément à l'article 33, paragraphes 2 à 4.

4. La Commission adopte des actes d'exécution pour établir les normes minimales en matière de qualité des données et les spécifications techniques visées aux paragraphes 1 et 3 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 33

Règles spécifiques pour les vérifications ou les recherches à l'aide de photographies, d'images faciales et de données dactyloscopiques

1. Lorsque des photographies, des images faciales et des données dactyloscopiques sont disponibles dans un signalement dans le SIS, ces photographies, images faciales et données dactyloscopiques sont utilisées pour confirmer l'identité d'une personne qui a été localisée à la suite d'une recherche alphanumérique effectuée dans le SIS.

2. Les données dactyloscopiques peuvent, dans tous les cas, faire l'objet de recherches pour identifier une personne. Toutefois, les données dactyloscopiques font l'objet de recherches pour identifier une personne lorsque l'identité de la personne ne peut pas être établie par d'autres moyens. À cette fin, le SIS central contient un système de reconnaissance automatisée d'empreintes digitales (AFIS).

3. Les données dactyloscopiques dans le SIS en rapport avec des signalements introduits conformément aux articles 24 et 25 peuvent également faire l'objet de recherches à l'aide de séries complètes ou incomplètes d'empreintes digitales ou d'empreintes palmaires découvertes sur les lieux d'infractions graves ou d'infractions terroristes faisant l'objet d'une enquête, lorsqu'il peut être établi, avec un degré élevé de probabilité, que ces séries d'empreintes appartiennent à un auteur de l'infraction et pour autant que les recherches soient effectuées simultanément dans les bases de données d'empreintes digitales nationales pertinentes de l'État membre.

4. Dès que cela est techniquement possible, et tout en assurant un haut degré de fiabilité de l'identification, les photographies et les images faciales peuvent être utilisées pour identifier une personne dans le contexte des points de passage frontaliers habituels.

Avant que cette fonctionnalité ne soit mise en œuvre dans le SIS, la Commission présente un rapport précisant si la technique requise est disponible, prête à être employée et fiable. Le Parlement européen est consulté sur ce rapport.

Après le début de l'utilisation de la fonctionnalité aux points de passage frontaliers habituels, la Commission est habilitée à adopter des actes délégués conformément à l'article 61 pour compléter le présent règlement en ce qui concerne la détermination des autres circonstances dans lesquelles des photographies et des images faciales peuvent être utilisées pour identifier des personnes.

CHAPITRE VII

DROIT D'ACCÈS, RÉEXAMEN ET SUPPRESSION DES SIGNALEMENTS

Article 34

Autorités nationales compétentes ayant un droit d'accès aux données dans le SIS

1. Les autorités nationales compétentes chargées de l'identification des ressortissants de pays tiers ont accès aux données introduites dans le SIS et ont le droit d'effectuer des recherches dans ces données, directement ou dans une copie de la base de données du SIS, aux fins:

a) du contrôle aux frontières, conformément au règlement (UE) 2016/399;

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) de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, et des enquêtes et des poursuites en la matière ou de l'exécution de sanctions pénales, dans l'État membre concerné, pour autant que la directive (UE) 2016/680 s'applique;

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 ce qui concerne les titres de séjour et les visas de long séjour, ainsi qu'au retour des ressortissants de pays tiers, de même qu'aux fins des vérifications portant sur les ressortissants de pays tiers qui entrent ou séjournent irrégulièrement sur le territoire des États membres;

e) des contrôles de sécurité portant sur les ressortissants de pays tiers qui demandent une protection internationale, dans la mesure où les autorités effectuant les contrôles ne sont pas des «autorités responsables de la détermination» au sens de l'article 2, point f), de la directive 2013/32/UE du Parlement européen et du Conseil ([1]), et, le cas échéant, aux fins de la fourniture de conseils conformément au règlement (CE) n° 377/2004 du Conseil ([2]);

f) de l'examen des demandes de visa et de l'adoption des décisions y relatives, notamment les décisions éventuelles d'annulation, d'abrogation ou de prolongation des visas, conformément au règlement (CE) n° 810/2009 du Parlement européen et du Conseil ([3]).

2. Le droit d'accès aux données dans le SIS et le droit d'effectuer des recherches directement dans ces données peuvent être exercés par les autorités nationales compétentes en matière de naturalisation, conformément au droit national, aux fins de l'examen d'une demande de naturalisation.

3. Aux fins des articles 24 et 25, le droit d'accès aux données dans le SIS et le droit d'effectuer des recherches directement dans ces données 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 pour mener les enquêtes judiciaires avant l'inculpation d'une personne, dans l'exercice de leurs fonctions, conformément au droit national, et par leurs autorités de coordination.

4. Le droit d'accès aux données concernant des documents relatifs à des personnes, introduites conformément à l'article 38, paragraphe 2, points k) et l), du règlement (UE) 2018/1862 et le droit d'effectuer des recherches dans ces données peuvent également être exercés par les autorités visées au paragraphe 1, point f), du présent article.

5. Les autorités compétentes visées au présent article sont incluses dans la liste mentionnée à l'article 41, paragraphe 8.

Article 35

Accès d'Europol aux données dans le SIS

1. L'Agence de l'Union européenne pour la coopération des services répressifs (Europol), établie par le règlement (UE) 2016/794, a, dans la mesure nécessaire à l'exécution de son mandat, le droit d'accès aux données dans le SIS et le droit d'effectuer des recherches dans ces données. Europol peut également échanger des informations supplémentaires et demander, en outre, des informations supplémentaires conformément aux dispositions du manuel SIRENE.

2. Lorsqu'une recherche effectuée par Europol révèle l'existence d'un signalement dans le SIS, Europol informe l'État membre signalant par la voie d'échange d'informations supplémentaires au moyen de l'infrastructure de communication et conformément aux dispositions prévues par le manuel SIRENE. Jusqu'à ce qu'Europol soit en mesure d'utiliser les fonctionnalités prévues pour l'échange d'informations supplémentaires, elle informe les États membres signalants par l'intermédiaire des canaux définis dans le règlement (UE) 2016/794.

3. Europol peut traiter les informations supplémentaires qui lui ont été communiquées par les États membres à des fins de comparaison avec ses bases de données et ses projets d'analyse opérationnelle, en vue d'établir des liens ou d'autres rapports pertinents ainsi qu'aux fins des analyses de nature stratégique ou thématique ou des analyses opérationnelles visées à l'article 18, paragraphe 2, points a), b) et c), du règlement (UE) 2016/794. Tout traitement d'informations supplémentaires par Europol aux fins du présent article est effectué conformément audit règlement.

4. L'utilisation par Europol des informations obtenues lors d'une recherche dans le SIS ou lors du traitement d'informations supplémentaires est soumise à l'accord de l'État membre signalant. Si ledit État membre autorise l'utilisation de ces informations, leur traitement par Europol est régi par le règlement (UE) 2016/794. Europol ne communique ces informations à des pays tiers et à des organismes tiers qu'avec le consentement de l'État membre signalant et dans le respect absolu du droit de l'Union relatif à la protection des données.

([1]) Directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale (JO L 180 du 29.6.2013, p. 60).

([2]) Règlement (CE) n° 377/2004 du Conseil du 19 février 2004 relatif à la création d'un réseau d'officiers de liaison «Immigration» (JO L 64 du 2.3.2004, p. 1).

([3]) Règlement (CE) n° 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).

5. Europol:

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

b) nonobstant l'article 31, paragraphe 1, du règlement (UE) 2016/794, supprime les informations supplémentaires comportant des données à caractère personnel au plus tard un an après que le signalement correspondant a été supprimé. À titre dérogatoire, lorsqu'Europol possède, dans ses bases de données ou dans ses projets d'analyse opérationnelle, des informations sur une affaire à laquelle les informations supplémentaires sont liées, afin de pouvoir s'acquitter de ses missions, Europol peut, à titre exceptionnel, continuer à conserver les informations supplémentaires, si nécessaire. Europol informe l'État membre signalant et l'État membre d'exécution du maintien de la conservation de ces informations supplémentaires, en justifiant celui-ci;

c) limite l'accès aux données dans le SIS, y compris les informations supplémentaires, au personnel expressément autorisé d'Europol qui demande l'accès à ces données pour l'exécution de ses missions;

d) adopte et applique des mesures pour garantir la sécurité, la confidentialité et l'autocontrôle conformément aux articles 10, 11 et 13;

e) veille à ce que son personnel qui est autorisé à traiter des données du SIS reçoive une formation et des informations appropriées conformément à l'article 14, paragraphe 1; et

f) sans préjudice du règlement (UE) 2016/794, autorise le Contrôleur européen de la protection des données à contrôler et à examiner les activités d'Europol dans le cadre de l'exercice de son droit d'accès aux données dans le SIS et de son droit d'effectuer des recherches dans ces données et dans le cadre de l'échange et du traitement d'informations supplémentaires.

6. Europol ne copie les données du SIS qu'à des fins techniques lorsque cette copie est nécessaire au personnel dûment autorisé d'Europol pour effectuer une recherche directe. Le présent règlement s'applique à ces copies. La copie technique n'est utilisée qu'à des fins de conservation des données du SIS pendant que ces données font l'objet de recherches. Les données sont supprimées une fois les recherches terminées. De telles utilisations ne sont pas considérées comme des téléchargements ou copies illicites de données du SIS. Europol s'abstient de copier les données d'un signalement ou des données complémentaires émanant des États membres, ou des données provenant du CS-SIS, vers d'autres systèmes d'Europol.

7. Aux fins de vérifier la licéité du traitement des données, d'assurer un autocontrôle et de garantir la sécurité et l'intégrité des données, Europol consigne dans des registres tout accès au SIS et toute recherche dans le SIS conformément aux dispositions de l'article 12. De tels registres et traces documentaires ne sont pas considérés comme des téléchargements ou copies illicites d'une partie du SIS.

8. Les États membres informent Europol, par la voie d'échange d'informations supplémentaires, de toute réponse positive à des signalements liés à des infractions terroristes. À titre exceptionnel, les États membres peuvent ne pas informer Europol si la transmission de ces informations compromettrait des enquêtes en cours ou la sécurité d'une personne physique, ou serait contraire aux intérêts essentiels de la sécurité de l'État membre signalant.

9. Le paragraphe 8 s'applique à partir de la date à laquelle Europol est en mesure de recevoir des informations supplémentaires conformément au paragraphe 1.

Article 36

Accès aux données dans le SIS par les équipes du corps européen de garde-frontières et de garde-côtes, les équipes d'agents intervenant dans les tâches liées au retour 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 visées à l'article 2, points 8) et 9), dudit règlement ont le droit, dans les limites de leur mandat et pour autant que ceux-ci soient autorisés à procéder à des vérifications conformément à l'article 34, paragraphe 1, du présent règlement et qu'ils aient reçu la formation requise conformément à l'article 14, paragraphe 1, du présent règlement, d'avoir accès aux données dans le SIS et d'effectuer des recherches dans ces données dans la mesure où cela est nécessaire à l'exécution de leurs missions et où cela est requis par le plan opérationnel pour une opération spécifique. L'accès aux données dans le SIS ne s'étend pas à d'autres membres des équipes.

2. Les membres des équipes visés au paragraphe 1 exercent le droit d'accès aux données dans le SIS et le droit d'effectuer des recherches dans ces données, conformément au paragraphe 1, par l'intermédiaire d'une interface technique. L'interface technique est créée et gérée par l'Agence européenne de garde-frontières et de garde-côtes et permet une connexion directe au SIS central.

3. Lorsqu'une recherche effectuée par un membre des équipes visé au paragraphe 1 du présent article révèle l'existence d'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 n'agissent en réaction à un signalement dans le SIS que sur les instructions et, en règle générale, en présence de garde-frontières ou d'agents intervenant 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. Aux fins de vérifier la licéité du traitement des données, d'assurer un autocontrôle et de garantir la sécurité et l'intégrité des données, l'Agence européenne de garde-frontières et de garde-côtes consigne dans des registres tout accès au SIS et toute recherche effectuée dans le SIS conformément aux dispositions de l'article 12.

5. L'Agence européenne de garde-frontières et de garde-côtes adopte et applique des mesures pour assurer la sécurité, la confidentialité et l'autocontrôle, conformément aux articles 10, 11 et 13, et veille à ce que les équipes visées au paragraphe 1 du présent article appliquent ces mesures.

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

7. Sans préjudice du paragraphe 2, aucune des parties du SIS n'est connectée à un système de collecte et de traitement des données exploité par les équipes visées au paragraphe 1 ou par l'Agence européenne de garde-frontières et de garde-côtes, et aucune des données dans le SIS auxquelles ces équipes ont accès n'est transférée vers un tel système. Aucune partie du SIS ne doit être téléchargée ou copiée. L'enregistrement dans un registre des accès et des recherches n'est pas considéré comme un téléchargement ou une copie illicite de données du SIS.

8. L'Agence européenne de garde-frontières et de garde-côtes autorise le Contrôleur européen de la protection des données à contrôler et à examiner les activités des équipes visées au présent article dans le cadre de l'exercice de leur droit d'accès aux données dans le SIS et de leur droit d'effectuer des recherches dans ces données. Cette disposition est sans préjudice des autres dispositions du règlement (UE) 2018/1725.

Article 37

Évaluation de l'utilisation du SIS par Europol et l'Agence européenne de garde-frontières et de garde-côtes

1. La Commission procède, au moins tous les cinq ans, à une évaluation de l'exploitation et de l'utilisation du SIS par Europol et les équipes visées à l'article 36, paragraphe 1.

2. Europol et l'Agence européenne de garde-frontières et de garde-côtes veillent à ce que des suites adéquates soient données aux conclusions et recommandations résultant de l'évaluation.

3. Un rapport sur les résultats de l'évaluation et les suites qui y sont données est transmis au Parlement européen et au Conseil.

Article 38

Limites d'accès

Les utilisateurs finaux, y compris Europol et les membres des équipes visés à l'article 2, points 8) et 9), du règlement (UE) 2016/1624, n'accèdent qu'aux données qui sont nécessaires à l'exécution de leurs missions.

Article 39

Délai de réexamen des signalements

1. Les signalements ne sont conservés que pendant le temps nécessaire à la réalisation des finalités pour lesquelles ils ont été introduits.

2. Un État membre signalant réexamine, dans un délai de trois ans à compter de l'introduction d'un signalement dans le SIS, la nécessité de l'y conserver. Cependant, si la décision nationale sur laquelle le signalement se fonde prévoit une durée de validité supérieure à trois ans, le signalement est réexaminé dans un délai de cinq ans.

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

4. L'État membre signalant peut, dans le délai de réexamen, décider, au terme d'une évaluation individuelle globale, qui est enregistrée, de conserver le signalement pour une durée plus longue que le délai de réexamen si cela s'avère nécessaire et proportionné aux fins pour lesquelles le signalement a été introduit. Dans ce cas, le paragraphe 2 s'applique également à la prolongation. Toute prolongation de ce type est communiquée au CS-SIS.

5. Les signalements sont automatiquement supprimés à l'expiration du délai de réexamen visé au paragraphe 2, sauf dans le cas où l'État membre signalant a informé le CS-SIS d'une prolongation en vertu du paragraphe 4. Le CS-SIS informe automatiquement l'État membre signalant de la suppression programmée de données avec un préavis de quatre mois.

6. Les États membres tiennent des statistiques sur le nombre de signalements dont la durée de conservation a été prolongée conformément au paragraphe 4 du présent article et les transmettent, sur demande, aux autorités de contrôle visées à l'article 55.

7. Dès qu'il est clair pour un bureau SIRENE que le signalement a atteint son objectif et devrait par conséquent être supprimé, il envoie immédiatement une notification à l'autorité qui a créé le signalement. L'autorité dispose d'un délai de 15 jours civils à compter de la réception de cette notification pour répondre que le signalement a été ou sera supprimé ou pour exposer les raisons de la conservation du signalement. Faute de réponse à l'expiration du délai de 15 jours, le bureau SIRENE veille à ce que le signalement soit supprimé. Si le droit national l'autorise, le signalement est supprimé par le bureau SIRENE. Les bureaux SIRENE signalent à leur autorité de contrôle tout problème récurrent qu'ils rencontrent quand ils agissent au titre du présent paragraphe.

Article 40

Suppression des signalements

1. Les signalements aux fins de non-admission et d'interdiction de séjour introduits en vertu de l'article 24 sont supprimés:

a) lorsque l'autorité compétente a retiré ou annulé la décision ayant fondé l'introduction du signalement; ou

b) s'il y a lieu, au terme de la procédure de consultation visée aux articles 27 et 29.

2. Les signalements concernant des ressortissants de pays tiers qui font l'objet d'une mesure restrictive visant à les empêcher d'entrer sur le territoire des États membres ou de transiter par ce territoire sont supprimés lorsque la mesure restrictive a pris fin, a été suspendue ou a été annulée.

3. Les signalements concernant une personne ayant acquis la citoyenneté d'un État membre ou d'un État dont les ressortissants sont bénéficiaires du droit de libre circulation au titre du droit de l'Union sont supprimés dès que l'État membre signalant apprend, ou est informé en application de l'article 44, que la personne concernée a acquis cette citoyenneté.

4. Les signalements sont supprimés dès l'expiration du signalement conformément à l'article 39.

CHAPITRE VIII

RÈGLES GÉNÉRALES RELATIVES AU TRAITEMENT DES DONNÉES

Article 41

Traitement des données du SIS

1. Les États membres ne traitent les données visées à l'article 20 qu'à des fins de non-admission et d'interdiction de séjour sur leur territoire.

2. Les données ne sont copiées qu'à des fins techniques, lorsque cette copie est nécessaire aux autorités compétentes visées à l'article 34 pour effectuer une recherche directe. Le présent règlement s'applique à ces copies. Tout État membre s'abstient de copier les données d'un signalement ou des données complémentaires introduites par un autre État membre depuis son N.SIS ou depuis le CS-SIS dans d'autres fichiers de données nationaux.

3. Les copies techniques visées au paragraphe 2 qui deviennent des bases de données hors ligne ne peuvent être conservées que pour une durée inférieure à 48 heures.

Nonobstant le premier alinéa, les copies techniques qui deviennent des bases de données hors ligne destinées à être utilisées par les 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 24 heures.

Les États membres tiennent à jour un inventaire de ces copies, le mettent à la disposition de leurs autorités de contrôle et veillent à ce que ces copies soient conformes au présent règlement, notamment à l'article 10.

4. L'accès aux données dans le SIS par les autorités nationales compétentes visées à l'article 34 est autorisé uniquement dans les limites de leurs compétences et est réservé au personnel dûment autorisé.

5. Tout traitement des données du SIS par les États membres 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 et imminente pour l'ordre public et la sécurité publique, pour des raisons graves de sécurité nationale ou aux fins de la prévention d'une infraction grave. À cette fin, l'autorisation préalable de l'État membre signalant doit être obtenue.

6. Les données concernant des documents relatifs à des personnes qui sont introduites dans le SIS conformément à l'article 38, paragraphe 2, points k) et l), du règlement (UE) 2018/1862 peuvent être utilisées par les autorités compétentes visées à l'article 34, paragraphe 1, point f), conformément à la législation de chaque État membre.

7. Toute utilisation de données du SIS qui ne respecte pas les paragraphes 1 à 6 du présent article est considérée comme une utilisation abusive au regard du droit national de chaque État membre et donne lieu à des sanctions conformément à l'article 59.

8. Chaque État membre communique à l'eu-LISA la liste de ses autorités compétentes autorisées à effectuer des recherches directement dans les données dans le SIS en vertu du présent règlement, ainsi que tout changement apporté à cette liste. La liste indique, pour chaque autorité, quelles données peuvent faire l'objet de recherches et à quelles fins. L'eu-LISA veille à ce que la liste soit publiée chaque année au *Journal officiel de l'Union européenne*. L'eu-LISA maintient sur son site internet une liste constamment mise à jour contenant les modifications transmises par les États membres entre les publications annuelles.

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 dans son N.SIS.

Article 42

Données du SIS et fichiers nationaux

1. L'article 41, paragraphe 2, est sans préjudice du droit qu'à un État membre de conserver, dans ses fichiers nationaux, des données du SIS sur la base desquelles la conduite 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 41, paragraphe 2, est sans préjudice du droit qu'à 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 43

Information en cas d'inexécution d'un signalement

Si une conduite demandée ne peut être exécutée, l'État membre requis pour cette conduite en informe directement l'État membre signalant par la voie d'échange d'informations supplémentaires.

Article 44

Qualité des données dans le SIS

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

2. Lorsqu'un État membre signalant reçoit des données complémentaires ou modifiées pertinentes telles qu'elles sont énumérées à l'article 20, paragraphe 2, il complète ou modifie sans tarder le signalement concerné.

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

4. Lorsqu'un État membre autre que l'État membre signalant dispose de données complémentaires ou modifiées pertinentes telles qu'elles sont énumérées à l'article 20, paragraphe 2, il les transmet sans tarder, par la voie d'échange d'informations supplémentaires, à l'État membre signalant afin de permettre à ce dernier de compléter ou de modifier le signalement. Les données ne sont transmises que si l'identité du ressortissant de pays tiers est établie.

5. Lorsqu'un État membre autre que l'État membre signalant dispose d'éléments de preuve suggérant qu'une donnée est matériellement erronée ou a été conservée de manière illicite, il en informe l'État membre signalant, par la voie d'échange d'informations supplémentaires, dans les meilleurs délais et au plus tard deux jours ouvrables après avoir relevé ces éléments de preuve. L'État membre signalant vérifie l'information et, s'il y a lieu, corrige ou supprime la donnée sans tarder.

6. Lorsque les États membres ne peuvent parvenir à un accord dans un délai de deux mois à compter de la découverte des éléments de preuve visés au paragraphe 5 du présent article, l'État membre qui n'a pas introduit le signalement soumet la question aux autorités de contrôle concernées et au Contrôleur européen de la protection des données aux fins de l'adoption d'une décision, par la voie de la coopération prévue à l'article 57.

7. Les États membres échangent des informations supplémentaires lorsqu'une personne se plaint de ne pas être la personne visée par un signalement. Lorsqu'il ressort des vérifications que la personne visée par un signalement n'est en réalité pas la personne qui s'est plainte, celle-ci est informée des mesures prévues à l'article 47 et du droit de recours dont elle dispose en vertu de l'article 54, paragraphe 1.

Article 45

Incidents de sécurité

1. Tout événement ayant ou pouvant avoir un impact sur la sécurité du SIS ou susceptible de causer des dommages ou des pertes aux données du SIS ou aux informations supplémentaires est considéré comme un incident de sécurité, en particulier lorsque des données peuvent avoir fait l'objet d'un accès illicite 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. Sans préjudice de la notification et de la communication d'une violation de données à caractère personnel en vertu de l'article 33 du règlement (UE) 2016/679 ou de l'article 30 de la directive (UE) 2016/680, les États membres, Europol et l'Agence européenne de garde-frontières et de garde-côtes informent sans tarder la Commission, l'eu-LISA, l'autorité de contrôle compétente et le Contrôleur européen de la protection des données des incidents de sécurité. L'eu-LISA informe sans tarder la Commission et le Contrôleur européen de la protection des données de tout incident de sécurité concernant le SIS central.

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'eu-LISA, sur la disponibilité, l'intégrité et la confidentialité des données introduites ou envoyées par d'autres États membres ou sur les informations supplémentaires échangées sont communiquées sans tarder à tous les États membres et signalées conformément au plan de gestion des incidents fourni par l'eu-LISA.

5. Les États membres et l'eu-LISA collaborent en cas d'incident de sécurité.

6. La Commission signale immédiatement les incidents graves au Parlement européen et au Conseil. Ces rapports sont classifiés EU RESTRICTED/RESTREINT UE conformément aux règles de sécurité applicables.

7. Lorsqu'un incident de sécurité a pour cause une utilisation abusive de données, les États membres, Europol et l'Agence européenne de garde-frontières et de garde-côtes veillent à ce que des sanctions soient imposées conformément à l'article 59.

Article 46

Différenciation des personnes présentant des caractéristiques similaires

1. Lorsque, lors de l'introduction d'un nouveau signalement, il apparaît qu'il existe déjà un signalement dans le SIS concernant une personne dont la description d'identité est la même, le bureau SIRENE contacte, dans un délai de 12 heures, l'État membre signalant par la voie d'échange d'informations supplémentaires pour vérifier si les personnes faisant l'objet des deux signalements sont la même personne.

2. Lorsque la vérification fait apparaître que la personne faisant l'objet du nouveau signalement et la personne faisant l'objet du signalement déjà introduit dans le SIS sont bien une seule et même personne, le bureau SIRENE applique la procédure concernant l'introduction de signalements multiples visée à l'article 23.

3. 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 données nécessaires pour éviter toute erreur d'identification.

Article 47

Données complémentaires pour traiter les cas d'usurpation d'identité

1. Lorsqu'il est possible de confondre la personne 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 conséquences négatives résultant d'une erreur d'identification. Toute personne dont l'identité a été usurpée a le droit de retirer son consentement en ce qui concerne le traitement des données à caractère personnel ajoutées.

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

a) permettre à l'autorité compétente de distinguer la personne dont l'identité a été usurpée de la personne visée par le signalement; et

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, et sous réserve du consentement explicite, pour chaque catégorie de données, de la personne dont l'identité a été usurpée, seules les données à caractère personnel de la personne dont l'identité a été usurpée énumérées ci-après peuvent être introduites dans le SIS et y faire l'objet d'un traitement ultérieur:

a) les noms;

b) les prénoms;

c) les noms 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 genre;

i) les photographies et les images faciales;

j) les empreintes digitales, les empreintes palmaires ou les deux;

k) toutes les nationalités possédées;

l) la catégorie des documents d'identification de la personne;

m) le pays de délivrance des documents d'identification de la personne;

n) le ou les numéros des documents d'identification de la personne;

o) la date de délivrance des documents d'identification de la personne;

p) l'adresse de la personne;

q) le nom du père de la personne;

r) le nom de la mère de la personne.

4. La Commission adopte des actes d'exécution pour établir et préciser les règles techniques nécessaires pour l'introduction et le traitement ultérieur des données visées au paragraphe 3 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

5. Les données visées 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 avoir accès aux données visées au paragraphe 3, et ce dans l'unique but d'éviter une erreur d'identification.

Article 48

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 signalements ou plus.

2. La mise en relation est sans effet sur la conduite particulière à tenir sur la base de chacun des signalements mis en relation, ou sur leur délai de réexamen.

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. La Commission adopte des actes d'exécution pour établir et préciser les règles techniques pour mettre en relation des signalements. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 49

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 finalités pour lesquelles elles ont été fournies. Elles sont, en tout état de cause, supprimées au plus tard un an après que le signalement correspondant a été supprimé du SIS.

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

Article 50

Transfert de données à caractère personnel à des tiers

Les données traitées dans le SIS et les informations supplémentaires y relatives échangées en vertu 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 51

Législation applicable

1. Le règlement (UE) 2018/1725 s'applique aux traitements de données à caractère personnel effectués par l'eu-LISA et l'Agence européenne de garde-frontières et de garde-côtes au titre du présent règlement. Le règlement (UE) 2016/794 s'applique aux traitements de données à caractère personnel effectués par Europol au titre du présent règlement.

2. Le règlement (UE) 2016/679 s'applique aux traitements de données à caractère personnel effectués, au titre du présent règlement, par les autorités compétentes visées à l'article 34 du présent règlement, exception faite des traitements de données 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 lorsque la directive (UE) 2016/680 s'applique.

Article 52

Droit à l'information

1. Les ressortissants de pays tiers qui font l'objet d'un signalement dans le SIS en sont informés conformément aux articles 13 et 14 du règlement (UE) 2016/679 ou aux articles 12 et 13 de la directive (UE) 2016/680. Cette information est fournie par écrit, avec une copie de la décision nationale qui est à l'origine du signalement visée à l'article 24, paragraphe 1, du présent règlement ou une référence à ladite décision.

2. Cette information n'est pas fournie lorsque le droit national permet de limiter le droit à l'information, en particulier pour préserver 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 53

Droit d'accès, de rectification des données inexactes et d'effacement de données conservées de manière illicite

1. Les personnes concernées ont la possibilité d'exercer les droits que leur confèrent les articles 15, 16 et 17 du règlement (UE) 2016/679 et l'article 14 et l'article 16, paragraphes 1 et 2, de la directive (UE) 2016/680.

2. Un État membre autre que l'État membre signalant ne peut fournir à la personne concernée des informations concernant l'une ou l'autre des données à caractère personnel de la personne concernée qui sont traitées que s'il donne d'abord à l'État membre signalant la possibilité de prendre position. La communication entre ces États membres se fait par la voie d'échange d'informations supplémentaires.

3. Un État membre peut décider de ne pas fournir des informations à la personne concernée, en tout ou en partie, conformément au droit national, dès lors et aussi longtemps qu'une limitation 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 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; ou

e) protéger les droits et libertés d'autrui.

Dans les cas visés au premier alinéa, l'État membre informe la personne concernée par écrit, sans retard indu, de tout refus ou de toute limitation d'accès, ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des motifs énoncés au premier alinéa, points a) à e). L'État membre informe la personne concernée de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

L'État membre documente les motifs de fait ou de droit sur lesquels se fonde la décision de ne pas fournir d'informations à la personne concernée. Ces informations sont mises à la disposition des autorités de contrôle.

Dans de tels cas, la personne concernée peut également exercer ses droits par l'intermédiaire des autorités de contrôle compétentes.

4. À la suite d'une demande d'accès, de rectification ou d'effacement, l'État membre informe la personne concernée dès que possible et, en tout état de cause, dans les délais visés à l'article 12, paragraphe 3, du règlement (UE) 2016/679, de la suite donnée à l'exercice des droits prévus au présent article, indépendamment du fait que la personne concernée se trouve ou non dans un pays tiers.

Article 54

Voies de recours

1. Sans préjudice des dispositions du règlement (UE) 2016/679 et de la directive (UE) 2016/680 relatives aux voies de recours, toute personne peut saisir toute autorité compétente, y compris une juridiction, en vertu du droit de tout État membre, afin d'avoir accès à des données, de faire rectifier ou d'effacer des données, d'obtenir des informations ou d'obtenir réparation en rapport avec 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 du présent article, sans préjudice de l'article 58.

3. Les États membres font rapport annuellement au comité européen de la protection des données sur:

a) le nombre de demandes d'accès présentées 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 à l'autorité de contrôle 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 conservées de manière illicite présentées au responsable du traitement et le nombre de cas où les données ont été rectifiées ou effacées;

d) le nombre de demandes de rectification de données inexactes et d'effacement de données conservées de manière illicite présentées à l'autorité de contrôle;

e) le nombre de procédures judiciaires engagées;

f) le nombre d'affaires dans lesquelles la juridiction saisie a statué en faveur du requérant;

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 introduits par l'État membre signalant.

La Commission établit un modèle pour la communication des informations visées au présent paragraphe.

4. Les rapports des États membres sont intégrés dans le rapport conjoint visé à l'article 57, paragraphe 4.

Article 55

Contrôle du N.SIS

1. Les États membres veillent à ce que les autorités de contrôle indépendantes désignées dans chaque État membre et investies des pouvoirs mentionnés au chapitre VI du règlement (UE) 2016/679 ou au chapitre VI de la directive (UE) 2016/680 contrôlent la licéité du traitement des données à caractère personnel dans le SIS sur leur territoire, leur transmission à partir de leur territoire et l'échange et le traitement ultérieur d'informations supplémentaires sur leur territoire.

2. Les autorités de contrôle veillent à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données dans le cadre de leur N.SIS, répondant aux normes internationales d'audit. Soit l'audit est réalisé par les autorités de contrôle, soit les autorités de contrôle commandent directement l'audit à un auditeur en matière de protection des données indépendant. En toutes circonstances, les autorités de contrôle conservent le contrôle de l'auditeur indépendant et assument la responsabilité des travaux de celui-ci.

3. Les États membres veillent à ce que leurs autorités de contrôle disposent des ressources nécessaires pour s'acquitter des tâches qui leur sont confiées par le présent règlement et puissent demander conseil à des personnes ayant des connaissances suffisantes en matière de données biométriques.

Article 56

Contrôle de l'eu-LISA

1. Le Contrôleur européen de la protection des données est chargé de contrôler le traitement des données à caractère personnel effectué par l'eu-LISA et de veiller à ce qu'il soit effectué conformément au présent règlement. Les tâches et pouvoirs visés aux articles 57 et 58 du règlement (UE) 2018/1725 s'appliquent en conséquence.

2. Le Contrôleur européen de la protection des données réalise, tous les quatre ans au minimum, un audit du traitement des données à caractère personnel effectué par l'eu-LISA, répondant aux normes internationales d'audit. Un rapport d'audit est communiqué au Parlement européen, au Conseil, à l'eu-LISA, à la Commission et aux autorités de contrôle. L'eu-LISA se voit offrir la possibilité de formuler des observations avant l'adoption du rapport.

Article 57

Coopération entre les autorités de contrôle et le Contrôleur européen de la protection des données

1. Les autorités de contrôle 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, les autorités de contrôle et le Contrôleur européen de la protection des données échangent les informations utiles, s'assistent mutuellement pour réaliser les audits et les inspections, examinent les difficultés d'interprétation ou d'application du présent règlement et d'autres actes juridiques applicables de l'Union, étudient les problèmes qui se sont 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 du paragraphe 2, les autorités de contrôle et le Contrôleur européen de la protection des données se réunissent au moins deux fois par an, dans le cadre du comité européen de la protection des données. Le coût et l'organisation de ces réunions sont à la charge du comité européen de la protection des données. 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 annuellement au Parlement européen, au Conseil et à la Commission par le comité européen de la protection des données.

CHAPITRE X

RESPONSABILITÉ ET SANCTIONS

Article 58

Responsabilité

1. Sans préjudice du droit à réparation et de toute responsabilité prévus par le règlement (UE) 2016/679, la directive (UE) 2016/680 et le règlement (UE) 2018/1725:

a) toute personne ou tout État membre ayant subi un dommage matériel ou immatériel du fait d'une opération illicite de traitement de données à caractère personnel dans le cadre du N.SIS ou de tout autre acte incompatible avec le présent règlement de la part d'un État membre a le droit d'obtenir réparation dudit État membre; et

b) toute personne ou tout État membre ayant subi un dommage matériel ou immatériel du fait de tout acte de l'eu-LISA incompatible avec le présent règlement a le droit d'obtenir réparation de l'eu-LISA.

Un État membre ou l'eu-LISA sont exonérés, totalement ou partiellement, de leur responsabilité prévue au premier alinéa s'ils prouvent que le fait générateur du dommage ne leur est pas imputable.

2. Lorsque le non-respect, par un État membre, des obligations qui lui incombent au titre du présent règlement cause un dommage au SIS, cet État membre en est tenu responsable, sauf si et dans la mesure où l'eu-LISA ou un autre État membre participant au SIS n'ont pas pris de mesures raisonnables pour prévenir le dommage ou en atténuer les effets.

3. Les actions en réparation intentées contre un État membre pour les dommages visés aux paragraphes 1 et 2 sont régies par le droit national de cet État membre. Les actions en réparation intentées contre l'eu-LISA pour les dommages visés aux paragraphes 1 et 2 sont soumises aux conditions prévues dans les traités.

Article 59

Sanctions

Les États membres veillent à ce que toute utilisation abusive des données du SIS ou tout traitement de ces données ou tout échange d'informations supplémentaires contraire au présent règlement soit punissable conformément au droit national.

Les sanctions prévues sont effectives, proportionnées et dissuasives.

CHAPITRE XI

DISPOSITIONS FINALES

Article 60

Suivi et statistiques

1. L'eu-LISA veille à ce que des procédures soient mises en place pour assurer le suivi du 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, de l'établissement de rapports, de rapports sur la qualité des données et de statistiques, l'eu-LISA a accès aux informations nécessaires concernant les opérations de traitement effectuées dans le SIS central.

3. L'eu-LISA publie des statistiques journalières, mensuelles et annuelles, présentant le nombre d'enregistrements par catégorie de signalements, ventilées par État membre et sous forme de totaux. L'eu-LISA établit également des rapports annuels sur le nombre de réponses positives par catégorie de signalements, le nombre de fois où le SIS a été consulté et où on a eu accès au système pour introduire, mettre à jour ou supprimer un signalement, ventilés par État membre et sous forme de totaux. Ces statistiques comprennent des statistiques sur les échanges d'informations au titre des articles 27 à 31. Les statistiques ne contiennent pas de données à caractère personnel. Le rapport statistique annuel est publié.

4. Les États membres, Europol et l'Agence européenne de garde-frontières et de garde-côtes communiquent à l'eu-LISA et à la Commission les informations nécessaires pour établir les rapports visés aux paragraphes 3, 5, 7 et 8.

5. L'eu-LISA communique au Parlement européen, au Conseil, aux États membres, à la Commission, à Europol, à l'Agence européenne de garde-frontières et de garde-côtes et au Contrôleur européen de la protection des données tout rapport statistique qu'elle produit.

Pour contrôler la mise en œuvre des actes juridiques de l'Union, y compris aux fins du règlement (UE) n° 1053/2013, la Commission peut demander à l'eu-LISA de fournir d'autres rapports statistiques spécifiques, réguliers ou ponctuels, sur la performance du SIS, l'utilisation du SIS et l'échange d'informations supplémentaires.

L'Agence européenne de garde-frontières et de garde-côtes peut demander à l'eu-LISA de fournir d'autres rapports statistiques spécifiques, réguliers ou ponctuels, aux fins de la réalisation des analyses des risques et des évaluations de la vulnérabilité prévues aux articles 11 et 13 du règlement (UE) 2016/1624.

6. Aux fins de l'article 15, paragraphe 4, et des paragraphes 3, 4 et 5 du présent article, l'eu-LISA crée, met en œuvre et héberge sur ses sites techniques un fichier central contenant les données visées à l'article 15, paragraphe 4, et au paragraphe 3 du présent article, qui ne permet pas l'identification des personnes mais permet à la Commission et aux agences visées au paragraphe 5 du présent article d'obtenir des rapports et statistiques sur mesure. Sur demande, l'eu-LISA donne aux États membres, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes, dans la mesure nécessaire à l'exécution de leurs missions, l'accès au fichier central, au moyen d'un accès sécurisé via l'infrastructure de communication. L'eu-LISA met en place des contrôles d'accès et des profils d'utilisateurs spécifiques pour garantir que l'accès au fichier central n'est possible qu'aux seules fins de l'établissement de rapports et de statistiques.

7. Deux ans après la date d'application du présent règlement en vertu de l'article 66, paragraphe 5, premier alinéa, puis tous les deux ans, l'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 leur sécurité, sur AFIS et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres. Ce rapport contient également, dès que la technologie est utilisée, une évaluation de l'utilisation des images faciales aux fins de l'identification des personnes.

8. Trois ans après la date d'application du présent règlement en vertu de l'article 66, paragraphe 5, premier alinéa, puis tous les quatre ans, la Commission réalise une 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. Le rapport d'évaluation comprend également une évaluation d'AFIS et des campagnes d'information sur le SIS réalisées par la Commission conformément à l'article 19.

Le rapport d'évaluation contient en outre des statistiques sur le nombre de signalements introduits conformément à l'article 24, paragraphe 1, point a), et des statistiques sur le nombre de signalements introduits conformément au point b) dudit paragraphe. En ce qui concerne les signalements relevant de l'article 24, paragraphe 1, point a), le rapport précise le nombre de signalements introduits à la suite des situations visées à l'article 24, paragraphe 2, point a), b) ou c). Il comporte par ailleurs une évaluation de l'application de l'article 24 par les États membres.

La Commission transmet le rapport d'évaluation au Parlement européen et au Conseil.

9. La Commission adopte des actes d'exécution pour établir et préciser les modalités de fonctionnement du fichier central visé au paragraphe 6 du présent article ainsi que les règles de protection et de sécurité des données applicables à ce fichier. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 62, paragraphe 2.

Article 61

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter les actes délégués visés à l'article 33, paragraphe 4, est conféré à la Commission pour une durée indéterminée à compter du 27 décembre 2018.

3. La délégation de pouvoir visée à l'article 33, paragraphe 4, peut être révoquée à tout moment par le Parlement européen ou par le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes énoncés dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 33, paragraphe 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 62

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

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

Article 63

Modifications du règlement (CE) nº 1987/2006

Le règlement (CE) nº 1987/2006 est modifié comme suit:

1) L'article 6 est remplacé par le texte suivant:

«*Article 6*

Systèmes nationaux

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

2. Chaque État membre assume la responsabilité de garantir aux utilisateurs finaux une disponibilité continue des données du SIS II.»

2) L'article 11 est remplacé par le texte suivant:

«*Article 11*

Confidentialité — États membres

1. Chaque État membre applique à l'égard de toutes les personnes et de tous les organismes appelés à travailler avec des données et des informations supplémentaires du SIS II ses règles en matière de 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.

2. Lorsqu'un État membre coopère avec des prestataires externes sur toute tâche liée au SIS II, il suit de près les activités des prestataires afin de veiller au respect de l'ensemble des dispositions du présent règlement, notamment en ce qui concerne la sécurité, la confidentialité et la protection des données.

3. La gestion opérationnelle des N.SIS II ou de copies techniques n'est en aucun cas confiée à une entreprise ou organisation privée.»

3) L'article 15 est modifié comme suit:

a) le paragraphe suivant est inséré:

«3 *bis*. L'instance gestionnaire élabore et gère un dispositif et des procédures de contrôle de qualité des données du CS-SIS. Elle présente à intervalles réguliers des rapports aux États membres à cet effet.

L'instance gestionnaire présente à la Commission à intervalles réguliers un rapport indiquant les problèmes rencontrés et les États membres concernés.

La Commission présente au Parlement européen et au Conseil, à intervalles réguliers, un rapport sur les problèmes rencontrés quant à la qualité des données.»;

b) le paragraphe 8 est remplacé par le texte suivant:

«8. La gestion opérationnelle du SIS II central comprend toutes les tâches nécessaires pour que le SIS II 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. Ces tâches incluent également la coordination, la gestion et le soutien des activités de test concernant le SIS II central et les N.SIS II, qui garantissent que le SIS II central et les N.SIS II fonctionnent conformément aux exigences de conformité technique fixées à l'article 9.»

4) À l'article 17, les paragraphes suivants sont ajoutés:

«3. Lorsque l'instance gestionnaire coopère avec des prestataires externes sur toute tâche liée au SIS II, elle suit de près les activités des prestataires afin de veiller au respect de l'ensemble des dispositions du présent règlement, notamment en ce qui concerne la sécurité, la confidentialité et la protection des données.

4. La gestion opérationnelle du CS-SIS n'est en aucun cas confiée à une entreprise ou organisation privée.»

5) À l'article 20, paragraphe 2, le point suivant est inséré:

«k *bis*) le type d'infraction;».

6) À l'article 21, l'alinéa suivant est ajouté:

«Lorsque la décision de non-admission et d'interdiction de séjour visée à l'article 24, paragraphe 2, est liée à une infraction terroriste, le cas est considéré comme étant suffisamment approprié, pertinent et important pour justifier un signalement dans le SIS II. Pour des raisons de sécurité publique ou nationale, les États membres peuvent, à titre exceptionnel, s'abstenir d'introduire un signalement si celui-ci risque de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires.»

7) L'article 22 est remplacé par le texte suivant:

«*Article 22*

Règles spécifiques pour l'introduction, la vérification ou les recherches à l'aide de photographies et d'empreintes digitales

1. Les photographies et les empreintes digitales ne sont introduites qu'après avoir été soumises à un contrôle de qualité spécial visant à établir si les normes minimales en matière de qualité ont été respectées. Les spécifications de ce contrôle de qualité spécial sont fixées conformément à la procédure visée à l'article 51, paragraphe 2.

2. Lorsque des photographies et des données dactyloscopiques sont disponibles dans un signalement introduit dans le SIS II, ces photographies et ces données dactyloscopiques sont utilisées pour confirmer l'identité d'une personne localisée à la suite d'une recherche alphanumérique effectuée dans le SIS II.

3. Les données dactyloscopiques peuvent, dans tous les cas, faire l'objet de recherches pour identifier une personne. Toutefois, les données dactyloscopiques font l'objet de recherches pour identifier une personne lorsque l'identité de la personne ne peut pas être établie par d'autres moyens. À cette fin, le SIS II central contient un système de reconnaissance automatisée d'empreintes digitales (AFIS).

4. Les données dactyloscopiques dans le SIS II en rapport avec des signalements introduits conformément aux articles 24 et 26 peuvent également faire l'objet de recherches à l'aide de séries complètes ou incomplètes d'empreintes digitales découvertes sur les lieux d'infractions graves ou d'infractions terroristes faisant l'objet d'une enquête, lorsqu'il peut être établi, avec un degré élevé de probabilité, que ces séries d'empreintes appartiennent à un auteur de l'infraction et pour autant que les recherches soient effectuées simultanément dans les bases de données d'empreintes digitales nationales pertinentes de l'État membre.»

8) L'article 26 est remplacé par le texte suivant:

«*Article 26*

Conditions d'introduction des signalements concernant les ressortissants de pays tiers qui font l'objet de mesures restrictives

1. Les signalements concernant les ressortissants de pays tiers qui font l'objet d'une mesure restrictive visant à les empêcher d'entrer sur le territoire des États membres ou de transiter par ce territoire, prise conformément à des actes juridiques adoptés par le Conseil, y compris les mesures mettant en œuvre une interdiction de voyager imposée par le Conseil de sécurité des Nations unies, font, dans la mesure où il est satisfait aux exigences en matière de qualité des données, l'objet d'une introduction dans le SIS aux fins de non-admission et d'interdiction de séjour.

2. Les signalements sont introduits, mis à jour et supprimés par l'autorité compétente de l'État membre qui exerce la présidence du Conseil de l'Union européenne au moment de l'adoption de la mesure. Si cet État membre n'a pas accès au SIS II ou aux signalements introduits conformément au présent règlement, la responsabilité est assumée par l'État membre qui exerce la présidence suivante et qui a accès au SIS II, y compris aux signalements introduits conformément au présent règlement.

Les États membres mettent en place les procédures nécessaires pour introduire, mettre à jour et supprimer ces signalements.»

9) Les articles suivants sont insérés:

«*Article 27* bis

Accès d'Europol aux données dans le SIS II

1. L'Agence de l'Union européenne pour la coopération des services répressifs (Europol), établie par le règlement (UE) 2016/794 du Parlement européen et du Conseil (*), a, dans la mesure nécessaire à l'exécution de son mandat, le droit d'accès aux données dans le SIS II et le droit d'effectuer des recherches dans ces données. Europol peut également échanger des informations supplémentaires et demander, en outre, des informations supplémentaires conformément aux dispositions du manuel SIRENE.

2. Lorsqu'une recherche effectuée par Europol révèle l'existence d'un signalement dans le SIS II, Europol informe l'État membre signalant par la voie d'échange d'informations supplémentaires au moyen de l'infrastructure de communication et conformément aux dispositions prévues par le manuel SIRENE. Jusqu'à ce qu'Europol soit en mesure d'utiliser les fonctionnalités prévues pour l'échange d'informations supplémentaires, elle informe les États membres signalants par l'intermédiaire des canaux définis dans le règlement (UE) 2016/794.

3. Europol peut traiter les informations supplémentaires qui lui ont été communiquées par les États membres à des fins de comparaison avec ses bases de données et ses projets d'analyse opérationnelle, en vue d'établir des liens ou d'autres rapports pertinents ainsi qu'aux fins des analyses de nature stratégique ou thématique ou des analyses opérationnelles visées à l'article 18, paragraphe 2, points a), b) et c), du règlement (UE) 2016/794. Tout traitement d'informations supplémentaires par Europol aux fins du présent article est effectué conformément audit règlement.

4. L'utilisation par Europol des informations obtenues lors d'une recherche dans le SIS II ou lors du traitement d'informations supplémentaires est soumise à l'accord de l'État membre signalant. Si ledit État membre autorise l'utilisation de ces informations, leur traitement par Europol est régi par le règlement (UE) 2016/794. Europol ne communique ces informations à des pays tiers et à des organismes tiers qu'avec le consentement de l'État membre signalant et dans le respect absolu du droit de l'Union relatif à la protection des données.

5. Europol:

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

b) nonobstant l'article 31, paragraphe 1, du règlement (UE) 2016/794, supprime les informations supplémentaires comportant des données à caractère personnel au plus tard un an après que le signalement correspondant a été supprimé. À titre dérogatoire, lorsqu'Europol possède, dans ses bases de données ou dans ses projets d'analyse opérationnelle, des informations sur une affaire à laquelle les informations supplémentaires sont liées, afin de pouvoir s'acquitter de ses missions, Europol peut, à titre exceptionnel, continuer à conserver les informations supplémentaires, si nécessaire. Europol informe l'État membre signalant et l'État membre d'exécution du maintien de la conservation de ces informations supplémentaires, en justifiant celui-ci;

c) limite l'accès aux données dans le SIS II, y compris les informations supplémentaires, au personnel expressément autorisé d'Europol qui demande l'accès à ces données pour l'exécution de ses missions;

d) adopte et applique des mesures pour garantir la sécurité, la confidentialité et l'autocontrôle conformément aux articles 10, 11 et 13;

e) veille à ce que son personnel qui est autorisé à traiter des données du SIS II reçoive une formation et des informations appropriées conformément à l'article 14; et

f) sans préjudice du règlement (UE) 2016/794, autorise le Contrôleur européen de la protection des données à contrôler et à examiner les activités d'Europol dans le cadre de l'exercice de son droit d'accès aux données dans le SIS II et de son droit d'effectuer des recherches dans ces données et dans le cadre de l'échange et du traitement d'informations supplémentaires.

6. Europol ne copie des données du SIS II qu'à des fins techniques lorsque cette copie est nécessaire au personnel dûment autorisé d'Europol pour effectuer une recherche directe. Le présent règlement s'applique à ces copies. La copie technique n'est utilisée qu'à des fins de conservation de données du SIS II pendant que ces données font l'objet de recherches. Les données sont supprimées une fois les recherches terminées. De telles utilisations ne sont pas considérées comme des téléchargements ou copies illicites de données du SIS II. Europol s'abstient de copier les données d'un signalement ou des données complémentaires émanant des États membres, ou des données provenant du CS-SIS II, vers d'autres systèmes d'Europol.

7. Aux fins de vérifier la licéité du traitement des données, d'assurer un autocontrôle et de garantir la sécurité et l'intégrité des données, Europol consigne dans des registres tout accès au SIS II et toute recherche dans le SIS II conformément aux dispositions de l'article 12. De tels registres et traces documentaires ne sont pas considérés comme des téléchargements ou copies illicites d'une partie du SIS II.

8. Les États membres informent Europol, par la voie d'échange d'informations supplémentaires, de toute réponse positive à des signalements liés à des infractions terroristes. À titre exceptionnel, les États membres peuvent ne pas informer Europol si la transmission de ces informations compromettrait des enquêtes en cours ou la sécurité d'une personne physique, ou serait contraire aux intérêts essentiels de la sécurité de l'État membre signalant.

9. Le paragraphe 8 s'applique à partir de la date à laquelle Europol est en mesure de recevoir des informations supplémentaires conformément au paragraphe 1.

Article 27 ter

Accès aux données dans le SIS II par les équipes du corps européen de garde-frontières et de garde-côtes, les équipes d'agents intervenant dans les tâches liées au retour 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 du Parlement européen et du Conseil (**), les membres des équipes visées à l'article 2, points 8) et 9), dudit règlement ont le droit, dans les limites de leur mandat et pour autant que ceux-ci soient autorisés à procéder à des vérifications conformément à l'article 27, paragraphe 1, du présent règlement et qu'ils aient reçu la formation requise conformément à l'article 14 du présent règlement, d'avoir accès aux données dans le SIS II et d'effectuer des recherches dans ces données dans la mesure où cela est nécessaire à l'exécution de leurs missions et où cela est requis par le plan opérationnel pour une opération spécifique. L'accès aux données dans le SIS II ne s'étend pas à d'autres membres des équipes.

2. Les membres des équipes visés au paragraphe 1 exercent le droit d'accès aux données dans le SIS II et le droit d'effectuer des recherches dans ces données, conformément au paragraphe 1, par l'intermédiaire d'une interface technique. L'interface technique est créée et gérée par l'Agence européenne de garde-frontières et de garde-côtes et permet une connexion directe au SIS II central.

3. Lorsqu'une recherche effectuée par un membre des équipes visé au paragraphe 1 du présent article révèle l'existence d'un signalement dans le SIS II, l'État membre signalant en est informé. Conformément à l'article 40 du règlement (UE) 2016/1624, les membres des équipes n'agissent en réaction à un signalement dans le SIS II que sur les instructions et, en règle générale, en présence de garde-frontières ou d'agents intervenant 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. Aux fins de vérifier la licéité du traitement des données, d'assurer un autocontrôle et de garantir la sécurité et l'intégrité des données, l'Agence européenne de garde-frontières et de garde-côtes consigne dans des registres tout accès au SIS II et toute recherche effectuée dans le SIS II conformément aux dispositions de l'article 12.

5. L'Agence européenne de garde-frontières et de garde-côtes adopte et applique des mesures pour assurer la sécurité, la confidentialité et l'autocontrôle, conformément aux articles 10, 11 et 13, et veille à ce que les équipes visées au paragraphe 1 du présent article appliquent ces mesures.

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

7. Sans préjudice du paragraphe 2, aucune des parties du SIS II n'est connectée à un système de collecte et de traitement des données exploité par les équipes visées au paragraphe 1 ou par l'Agence européenne de garde-frontières et de garde-côtes, et aucune des données dans le SIS II auxquelles ces équipes ont accès n'est transférée vers un tel système. Aucune partie du SIS II ne doit être téléchargée ou copiée. L'enregistrement dans un registre des accès et des recherches n'est pas considéré comme un téléchargement ou une copie illicite de données du SIS II.

8. L'Agence européenne de garde-frontières et de garde-côtes autorise le Contrôleur européen de la protection des données à contrôler et à examiner les activités des équipes visées au présent article dans le cadre de l'exercice de leur droit d'accès aux données dans le SIS II et de leur droit d'effectuer des recherches dans ces données. Cette disposition est sans préjudice des autres dispositions du règlement (UE) 2018/1725 du Parlement européen et du Conseil (***).

(*) 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 24.5.2016, p. 53).

(**) 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) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil (JO L 251 du 16.9.2016, p. 1).

(***) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).»

Article 64

Modification de la convention d'application de l'accord de Schengen

L'article 25 de la convention d'application de l'accord de Schengen est supprimé.

Article 65

Abrogation

Le règlement (CE) nº 1987/2006 est abrogé à partir de la date d'application du présent règlement prévue à l'article 66, paragraphe 5, premier alinéa.

Les références faites au règlement abrogé s'entendent comme faites au présent règlement et sont à lire selon le tableau de correspondance figurant en annexe.

Article 66

Entrée en vigueur, mise en service et application

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

2. Au plus tard le 28 décembre 2021, la Commission adopte une décision fixant la date à laquelle le SIS est mis en service en vertu du présent règlement, après avoir vérifié que les conditions suivantes sont remplies:

a) les actes d'exécution nécessaires à l'application du présent règlement ont été adoptés;

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; et

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

3. La Commission surveille étroitement le processus de réalisation progressive des conditions énoncées au paragraphe 2 et informe le Parlement européen et le Conseil du résultat de la vérification visée audit paragraphe.

4. Au plus tard le 28 décembre 2019 puis chaque année jusqu'à l'adoption par la Commission de la décision visée au paragraphe 2, la Commission présente au Parlement européen et au Conseil un rapport sur l'état d'avancement des préparations pour la mise en œuvre complète du présent règlement. Ce rapport contient également des informations détaillées sur les coûts encourus ainsi que des informations relatives à tout risque susceptible d'avoir des retombées sur les coûts totaux.

5. Le présent règlement s'applique à partir de la date déterminée conformément au paragraphe 2.

Par dérogation au premier alinéa:

a) l'article 4, paragraphe 4, l'article 5, l'article 8, paragraphe 4, l'article 9, paragraphes 1 et 5, l'article 15, paragraphe 7, l'article 19, l'article 20, paragraphes 3 et 4, l'article 32, paragraphe 4, l'article 33, paragraphe 4, l'article 47, paragraphe 4, l'article 48, paragraphe 6, l'article 60, paragraphes 6 et 9, l'article 61, l'article 62, l'article 63, points 1) à 6) et point 8), ainsi que les paragraphes 3 et 4 du présent article, s'appliquent à partir de la date d'entrée en vigueur du présent règlement;

b) l'article 63, point 9), s'applique à partir du 28 décembre 2019;

c) l'article 63, point 7), s'applique à partir du 28 décembre 2020.

6. La décision de la Commission visée au paragraphe 2 est publiée au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Bruxelles, le 28 novembre 2018.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	K. EDTSTADLER

ANNEXE

TABLEAU DE CORRESPONDANCE

Règlement (CE) nº 1987/2006	Le présent règlement
Article 1er	Article 1er
Article 2	Article 2
Article 3	Article 3
Article 4	Article 4
Article 5	Article 5
Article 6	Article 6
Article 7	Article 7
Article 8	Article 8
Article 9	Article 9
Article 10	Article 10
Article 11	Article 11
Article 12	Article 12
Article 13	Article 13
Article 14	Article 14
Article 15	Article 15
Article 16	Article 16
Article 17	Article 17
Article 18	Article 18
Article 19	Article 19
Article 20	Article 20
Article 21	Article 21
Article 22	Articles 32 et 33
Article 23	Article 22
—	Article 23
Article 24	Article 24
Article 25	Article 26
Article 26	Article 25
—	Article 27
—	Article 28
—	Article 29
—	Article 30
—	Article 31
Article 27	Article 34
Article 27 *bis*	Article 35
Article 27 *ter*	Article 36
—	Article 37
Article 28	Article 38
Article 29	Article 39
Article 30	Article 40
Article 31	Article 41

Règlement (CE) nº 1987/2006	Le présent règlement
Article 32	Article 42
Article 33	Article 43
Article 34	Article 44
—	Article 45
Article 35	Article 46
Article 36	Article 47
Article 37	Article 48
Article 38	Article 49
Article 39	Article 50
Article 40	—
—	Article 51
Article 41	Article 53
Article 42	Article 52
Article 43	Article 54
Article 44	Article 55
Article 45	Article 56
Article 46	Article 57
Article 47	—
Article 48	Article 58
Article 49	Article 59
Article 50	Article 60
—	Article 61
Article 51	Article 62
Article 52	—
—	Article 63
—	Article 64
Article 53	—
—	Article 65
Article 54	—
Article 55	Article 66