III

(Actes pris en application du traité UE)

ACTES PRIS EN APPLICATION DU TITRE VI DU TRAITÉ UE

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)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 30, paragraphe 1, points a) et b), son article 31, paragraphe 1, points a) et b), et son article 34, paragraphe 2, point c),

vu la proposition de la Commission,

vu l'avis du Parlement européen [1],

considérant ce qui suit:

(1) Le système d'information Schengen (le «SIS»), créé conformément aux dispositions du titre IV de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, signée le 19 juin 1990 [2] («convention de Schengen») et son développement, le SIS 1+, constituent un outil essentiel pour l'application des dispositions de l'acquis de Schengen, intégré dans le cadre de l'Union européenne.

(2) La Commission a été chargée du développement du SIS de deuxième génération (le «SIS II») par le règlement (CE) n° 2424/2001 du Conseil [3] et la décision 2001/886/JAI du Conseil du 6 décembre 2001 relatifs au développement du système d'information de Schengen de deuxième génération (SIS II) [4]. Le SIS II remplacera le SIS tel que créé par la convention de Schengen.

(3) La présente décision constitue la base législative requise pour régir le SIS II dans les domaines relevant du traité sur l'Union européenne (le «traité UE»). Le règlement (CE) n° 2006/1987 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du SIS II [5] constitue la base législative requise pour régir le SIS II dans les domaines relevant du traité instituant la Communauté européenne (le «traité CE»).

(4) Le fait que la base législative requise pour régir le SIS II comporte deux instruments séparés n'affecte pas le principe selon lequel le SIS II constitue un système d'information unique qui devrait fonctionner en tant que tel. Certaines dispositions de ces instruments devraient par conséquent être identiques.

(5) Le SIS II devrait constituer une mesure compensatoire qui contribue au maintien d'un niveau élevé de sécurité dans un espace de liberté, de sécurité et de justice de l'Union européenne par le soutien qu'il apporte à la coopération opérationnelle en matière pénale entre les services de police et les autorités judiciaires.

[1] Avis du 25 octobre 2006 (non encore publié au Journal officiel).

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

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

[4] JO L 328 du 13.12.2001, p. 1.

[5] JO L 381 du 28.12.2006, p. 4.

(6) Il est nécessaire de préciser les objectifs du SIS II, son architecture technique et de financement, de fixer des règles concernant son fonctionnement, son utilisation et de définir les responsabilités y afférentes, ainsi que les catégories de données à introduire dans le système, les finalités et les critères de leur introduction, les autorités qui sont autorisées à y avoir accès, la mise en relation des signalements, de même que des règles complémentaires concernant le traitement des données et la protection des données à caractère personnel.

(7) Le SIS II comprendra un système central (SIS II central) et des applications nationales. Les dépenses liées au fonctionnement du SIS II central et de l'infrastructure de communication devraient être inscrites au budget général de l'Union européenne.

(8) Il est nécessaire de rédiger un manuel qui contiendrait des règles détaillées sur l'échange de certaines informations supplémentaires concernant la conduite à observer à la suite de signalements. Les autorités nationales de chaque État membre devraient assurer cet échange d'informations.

(9) Pendant une période transitoire, la Commission devrait être chargée de la gestion opérationnelle du SIS II central et de différentes parties de l'infrastructure de communication. Elle peut néanmoins, afin d'assurer une transition en douceur vers le SIS II, déléguer ces responsabilités ou certaines d'entre elles à deux organismes publics nationaux. À long terme, à la suite d'une analyse d'impact comprenant une analyse approfondie des solutions de remplacement d'un point de vue financier, opérationnel et organisationnel et de propositions législatives de la Commission, il conviendrait de mettre en place une instance gestionnaire qui sera chargée de ces tâches. La période transitoire ne devrait pas dépasser cinq ans à compter de la date à partir de laquelle la présente décision s'appliquera.

(10) Le SIS contiendra des signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise et en vue d'une arrestation aux fins d'extradition. Outre les signalements, il convient de prévoir l'échange d'informations supplémentaires nécessaires aux procédures de remise et d'extradition. En particulier, les données visées à l'article 8 de la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres [1] devraient être traitées dans le cadre du SIS II.

(11) Il faudrait prévoir la possibilité d'ajouter dans le SIS II une traduction des données complémentaires introduites aux fins de remise en vertu d'un mandat d'arrêt européen et aux fins d'extradition.

(12) Le SIS II devrait contenir des signalements concernant des personnes disparues, dans l'intérêt de leur propre protection ou pour la prévention de menaces, concernant des personnes recherchées dans le cadre d'une procédure judiciaire concernant des personnes ou des objets aux fins de contrôle discret ou de contrôle spécifique, ainsi que concernant des objets aux fins d'une saisie ou de la preuve dans une procédure pénale.

(13) Les signalements ne devraient pas être conservés dans le SIS II pour une durée plus longue que le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été fournis. En principe, les signalements relatifs aux personnes devraient être automatiquement effacés du SIS II après trois ans. Les signalements relatifs aux objets, introduits aux fins de contrôle discret ou de contrôle spécifique, devraient être automatiquement effacés du SIS II après cinq ans. Les signalements relatifs aux objets, introduits aux fins d'une saisie ou de la preuve dans une procédure pénale, devraient être automatiquement effacés du SIS II après dix ans. La décision de conserver des signalements relatifs aux personnes devrait se fonder sur une évaluation individuelle complète. Les États membres devraient réexaminer les signalements relatifs aux personnes dans le délai défini et tenir des statistiques concernant le nombre de signalements relatifs aux personnes dont la durée de conservation a été prolongée.

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

(15) Il faudrait prévoir la possibilité pour un État membre d'apposer sur le signalement une mention, appelée «indicateur de validité», tendant à ce que la conduite à tenir qui est demandée dans le signalement ne soit pas exécutée sur son territoire. Lorsque des signalements sont effectués en vue d'une arrestation aux fins de remise, rien dans la présente décision ne devrait être interprété comme dérogeant aux dispositions de la décision-cadre 2002/584/JAI ou comme en empêchant l'application. La décision d'apposer un indicateur de validité sur un signalement ne devrait être fondée que sur les motifs de refus prévus dans ladite décision-cadre.

(16) Lorsqu'un indicateur de validité a été apposé et que le lieu où se trouve la personne recherchée en vue d'une arrestation aux fins de remise vient à être connu, ce lieu devrait toujours être communiqué à l'autorité judiciaire d'émission, celle-ci pouvant décider de transmettre un mandat d'arrêt européen à l'autorité judiciaire compétente conformément aux dispositions de la décision-cadre 2002/584/JAI.

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

[1] JO L 190 du 18.7.2002, p. 1.

(18) Les données traitées dans le SIS II en application de la présente décision ne devraient pas être transférées à un pays tiers ou à une organisation internationale ni mises à leur disposition. Néanmoins, il convient de renforcer la coopération entre l'Union européenne et Interpol en encourageant un échange efficace de données relatives aux passeports. Lorsque des données à caractère personnel sont transférées du SIS II à Interpol, celles-ci devraient bénéficier d'un niveau de protection adéquat, garanti par un accord et accompagné de garanties et de conditions strictes.

(19) Tous les États membres ont ratifié la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. L'article 9 de cette convention fixe des exceptions et des restrictions aux droits et obligations qu'elle prévoit, dans certaines limites. Les données à caractère personnel traitées dans le cadre de la mise en œuvre de la présente décision doivent être protégées conformément aux principes consacrés dans ladite convention. Ces principes doivent, le cas échéant, être complétés ou précisés dans la présente décision.

(20) Les principes énoncés dans la recommandation n° R (87)15 du comité des ministres du Conseil de l'Europe du 17 septembre 1987 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police devraient être pris en compte lorsque les services de police traitent des données à caractère personnel en application de la présente décision.

(21) La Commission a présenté au Conseil une proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, qui devrait être approuvée avant la fin de 2006 et s'appliquer aux données à caractère personnel traitées dans le cadre du système d'information Schengen de deuxième génération, ainsi qu'à l'échange d'informations supplémentaires qui y est lié effectué conformément à la présente décision.

(22) Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [1], et notamment ses dispositions relatives respectivement à la confidentialité et à la sécurité des traitements, s'applique au traitement des données à caractère personnel par des institutions ou organes communautaires dans l'exercice de leurs missions en tant que responsables de la gestion opérationnelle du SIS II, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire. Une partie du traitement des données à caractère personnel figurant dans le SIS II relève effectivement du champ d'application du droit communautaire. Pour une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel, il convient de préciser que, lorsque la Commission traite des données à caractère personnel en application de la présente décision, le règlement (CE) n° 45/2001 s'applique. Les principes consacrés par le règlement (CE) n° 45/2001 devraient, le cas échéant, être complétés ou précisés dans la présente décision.

(23) En ce qui concerne la confidentialité, les dispositions pertinentes du statut des fonctionnaires des Communautés européennes et du régime applicable aux autres agents des Communautés européennes devraient s'appliquer aux fonctionnaires et autres agents des Communautés européennes employés et travaillant en liaison avec le SIS II.

(24) Il convient que les autorités de contrôle nationales vérifient la licéité du traitement, par les États membres, des données à caractère personnel, tandis que le Contrôleur européen de la protection des données, nommé en vertu de la décision 2004/55/CE du Parlement européen et du Conseil du 22 décembre 2003 portant nomination de l'autorité de contrôle indépendante prévue à l'article 286 du traité CE [2], devrait contrôler les activités des institutions et organes communautaires en rapport avec le traitement de données à caractère personnel, en tenant compte des tâches limitées des institutions et organes communautaires en ce qui concerne les données elles-mêmes.

(25) Tant les États membres que la Commission devraient élaborer un plan de sécurité visant à faciliter une mise en œuvre effective des obligations en matière de sécurité, ainsi que coopérer de manière à traiter les questions de sécurité dans une perspective commune.

(26) Les dispositions en matière de protection des données contenues dans la convention du 26 juillet 1995 portant création d'un Office européen de police [3] (ci-après dénommée «convention Europol») s'appliquent au traitement des données du SIS II par Europol, notamment celles concernant le pouvoir qu'a l'autorité de contrôle commune instituée par la convention Europol de surveiller l'activité de cet office et celles concernant la responsabilité découlant de tout traitement illicite par Europol de données à caractère personnel.

(27) Les dispositions en matière de protection des données contenues dans la décision 2002/187/JAI du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité [4] s'appliquent au traitement des données du SIS II par Eurojust, notamment celles concernant le pouvoir qu'a l'organe de contrôle commun créé par cette décision de contrôler les activités d'Eurojust et celles concernant la responsabilité découlant de tout traitement non autorisé par Eurojust de données à caractère personnel.

[1] JO L 8 du 12.1.2001, p. 1.

[2] JO L 12 du 17.1.2004, p. 47.

[3] JO C 316 du 27.11.1995, p. 2.

[4] JO L 63 du 6.3.2002, p. 1.

(28) Pour assurer la transparence, la Commission ou, lorsqu'elle a été instituée, l'instance gestionnaire, devrait présenter tous les deux ans un rapport sur le fonctionnement technique du SIS II central et de l'infrastructure de communication, y compris la sécurité qu'elle offre, et sur les échanges d'informations supplémentaires. La Commission devrait procéder à une évaluation globale tous les quatre ans.

(29) De par leur nature technique, leur niveau de précision et la nécessité d'effectuer des mises à jour à intervalles réguliers, certains aspects du SIS II, notamment les règles techniques concernant l'introduction de données, y compris de données nécessaires à l'introduction de signalements, les mises à jour, les suppressions et les consultations, les règles de compatibilité et de priorité entre les signalements, l'apposition d'indicateurs de validité, la mise en relation des signalements et l'échange d'informations supplémentaires, ne peuvent être couverts de manière exhaustive par les dispositions de la présente décision. Les compétences d'exécution relatives à ces aspects devraient par conséquent être déléguées à la Commission. Les règles techniques concernant les consultations de signalements devraient tenir compte du bon fonctionnement des applications nationales. Sous réserve d'une analyse d'impact lancée par la Commission, on décidera de la mesure dans laquelle les mesures d'application pourraient relever de la responsabilité de l'instance gestionnaire, dès sa mise en place.

(30) La présente décision devrait définir la procédure par laquelle les mesures nécessaires à sa mise en œuvre seront adoptées. La procédure d'adoption des mesures d'application à arrêter en vertu de la présente décision et en vertu du règlement (CE) n° 1987/2006 devrait être identique.

(31) Il convient d'arrêter des dispositions transitoires pour ce qui est des signalements effectués dans le SIS 1+ qui doivent être transférés au SIS II. Certaines dispositions de l'acquis de Schengen devraient continuer à s'appliquer pendant une période limitée, jusqu'à ce que les États membres aient examiné la compatibilité des signalements avec le nouveau cadre juridique. La compatibilité des signalements relatifs aux personnes devrait être examinée en priorité. De plus, toute modification, tout ajout, toute correction ou toute mise à jour d'un signalement transféré du SIS 1+ au SIS II, ainsi que toute réponse positive à un tel signalement, devrait déclencher un examen immédiat de sa compatibilité avec les dispositions de la présente décision.

(32) Il est nécessaire de prévoir des dispositions spécifiques concernant le reliquat du budget affecté aux activités du SIS qui ne fait pas partie du budget général de l'Union européenne.

(33) Étant donné que les objectifs de l'action envisagée, à savoir l'établissement d'un système d'information commun et la fixation de règles applicables à ce dernier, ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de cette action, être mieux réalisés au niveau de l'Union européenne, le Conseil peut arrêter des mesures, conformément au principe de subsidiarité tel qu'énoncé à l'article 5 du traité CE et mentionné à l'article 2 du traité UE. Conformément au principe de proportionnalité énoncé à l'article 5 du traité CE, la présente décision n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(34) La présente décision respecte les droits fondamentaux et observe les principes reconnus, notamment, par la charte des droits fondamentaux de l'Union européenne.

(35) Le Royaume-Uni participe à la présente décision conformément à l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne annexé au traité UE et au traité CE et à l'article 8, paragraphe 2, de la décision 2000/365/CE 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 [1].

(36) L'Irlande participe à la présente décision conformément à l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne annexé au traité UE et au traité CE et à l'article 6, paragraphe 2, de la décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen [2].

(37) La présente décision est sans préjudice des modalités de participation partielle du Royaume-Uni et de l'Irlande à l'acquis de Schengen, telles qu'elles sont définies respectivement dans les décisions 2000/365/CE et 2002/192/CE.

(38) En ce qui concerne l'Islande et la Norvège, la présente décision 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 relève du domaine visé à l'article 1er, point G, de la décision 1999/437/CE du Conseil du 17 mai 1999 [4] relative à certaines modalités d'application de cet accord.

(39) Il y a lieu de conclure un arrangement pour permettre à des représentants de l'Islande et de la Norvège d'être associés aux travaux des comités assistant la Commission dans l'exercice de ses compétences d'exécution. Un tel arrangement a été envisagé dans l'échange de lettres entre le Conseil de l'Union européenne et la République d'Islande et le Royaume de Norvège concernant les comités qui assistent la Commission européenne dans l'exercice de ses pouvoirs exécutifs [5], qui est annexé à l'accord susvisé.

[1] JO L 131 du 1.6.2000, p. 43.
[2] JO L 64 du 7.3.2002, p. 20.
[3] JO L 176 du 10.7.1999, p. 36.
[4] JO L 176 du 10.7.1999, p. 31.
[5] JO L 176 du 10.7.1999, p. 53.

(40) En ce qui concerne la Suisse, la présente décision 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, qui relèvent des domaines visés à l'article 1er, point G, de la décision 1999/437/CE lu en liaison avec l'article 4, paragraphe 1, des décisions 2004/849/CE [1] et 2004/860/CE [2] du Conseil.

(41) Il y a lieu de conclure un arrangement pour permettre à des représentants de la Suisse d'être associés aux travaux des comités assistant la Commission dans l'exercice de ses compétences d'exécution. Un tel arrangement a été envisagé dans l'échange de lettres entre la Communauté et la Suisse, qui est annexé à l'accord susvisé.

(42) La présente décision 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 et de l'article 4, paragraphe 2, de l'acte d'adhésion de 2005.

(43) La présente décision devrait s'appliquer au Royaume-Uni, à l'Irlande et à la Suisse à des dates fixées conformément aux procédures prévues dans les instruments pertinents concernant l'application de l'acquis de Schengen aux États précités,

DÉCIDE:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Établissement et objectif général du SIS II

1. Il est institué par la présente un système d'information Schengen de deuxième génération (le «SIS II»).

2. L'objet du SIS II, conformément aux dispositions de la présente décision, est d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, ainsi que d'appliquer les dispositions du titre IV, chapitre 3, du traité relatives à la libre circulation des personnes sur les territoires des États membres, à l'aide des informations transmises par ce système.

Article 2

Champ d'application

1. La présente décision établit les conditions et les procédures relatives à l'introduction et au traitement dans le SIS II des signalements concernant des personnes ou des objets, ainsi qu'à l'échange d'informations supplémentaires et de données complémentaires aux fins de la coopération policière et judiciaire en matière pénale.

2. La présente décision contient également des dispositions relatives, en particulier, à l'architecture technique du SIS II, aux responsabilités incombant aux États membres et à l'instance gestionnaire visée à l'article 15, à des règles générales sur le traitement des données, aux droits des personnes concernées et à la responsabilité.

Article 3

Définitions

1. Aux fins de la présente décision, on entend par:

a) «signalement», un ensemble de données introduites dans le SIS II pour permettre aux autorités compétentes d'identifier une personne ou un objet en vue de tenir une conduite particulière à son égard;

b) «informations supplémentaires», les informations non stockées dans le SIS II, mais en rapport avec des signalements introduits dans le SIS II, qui doivent être échangées:

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

   ii) à la suite d'une réponse positive afin que la conduite à tenir appropriée puisse être exécutée;

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

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

   v) en ce qui concerne la compatibilité et la priorité des signalements;

   vi) en ce qui concerne les droits d'accès;

c) «données complémentaires», les données stockées dans le SIS II et en rapport avec des signalements introduits dans le SIS II, qui sont immédiatement accessibles aux autorités compétentes lorsque des personnes au sujet desquelles des données ont été introduites dans le SIS II («personne concernée») sont trouvées à la suite de consultations effectuées dans ce système;

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

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

d) «données à caractère personnel», toute information concernant une personne physique identifiée ou identifiable («personne concernée»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement;

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

2. Toute référence, dans la présente décision, à des dispositions de la décision-cadre 2002/584/JAI est réputée inclure les dispositions correspondantes des accords conclus entre l'Union européenne et des pays tiers sur la base des articles 24 et 38 du traité aux fins de la remise de personnes sur la base d'un mandat d'arrêt, qui prévoient la transmission d'un tel mandat d'arrêt par le biais du système d'information Schengen.

Article 4

Architecture technique et mode de fonctionnement du SIS II

1. Le SIS II se compose:

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

— une fonction de support technique (le «CS-SIS») contenant une base de données, la «base de données du SIS II»,

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

b) d'une section nationale (le «N.SIS II») dans chaque État membre, constituée des systèmes de données nationaux reliés au SIS II central. Un N.SIS II peut contenir un fichier de données (une «copie nationale») comportant une copie complète ou partielle de la base de données du SIS II;

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

2. Les données du SIS II sont introduites, mises à jour, supprimées et consultées par le biais des différents systèmes N.SIS II. Une copie nationale est disponible pour effectuer des interrogations automatisées sur le territoire de chacun des États membres utilisant une telle copie. Il n'est pas possible de consulter les fichiers de données des N.SIS II des autres États membres.

3. Le CS-SIS, qui assure le contrôle et la gestion techniques, est installé à Strasbourg (France) et un CS-SIS de secours, capable d'assurer l'ensemble des fonctionnalités du CS-SIS principal en cas de défaillance de celui-ci, est installé à Sankt Johann im Pongau (Autriche).

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

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

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

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

Article 5

Coûts

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

2. Ces coûts comprennent les travaux effectués dans le cadre du CS-SIS qui permettent d'assurer la fourniture des services visés à l'article 4, paragraphe 4.

3. Les coûts de mise en place, d'exploitation et de maintenance de chaque N.SIS II 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 et d'exploiter son N.SIS II, d'en assurer la maintenance et de connecter son N.SIS II à la NI-SIS.

Article 7

Office N.SIS II et bureau Sirene

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

Cette instance est responsable du bon fonctionnement et de la sécurité du N.SIS II, fait en sorte que les autorités compétentes aient accès au SIS II et prend les mesures nécessaires pour assurer le respect des dispositions de la présente décision.

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

2. Chaque État membre désigne l'instance chargée de l'échange de toutes les informations supplémentaires (le «bureau Sirene»), conformément aux dispositions du manuel Sirene, tel que visé à l'article 8.

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

3. Les États membres communiquent à l'instance gestionnaire les coordonnées de leur office N.SIS II et de leur bureau Sirene. L'instance gestionnaire publie la liste de ces coordonnées ainsi que celle visée à l'article 46, paragraphe 8.

Article 8

Échange d'informations supplémentaires

1. Les informations supplémentaires sont échangées conformément aux dispositions d'un manuel appelé «le manuel Sirene» et au moyen de l'infrastructure de communication. Au cas où l'infrastructure de communication ne serait pas accessible, les États membres peuvent utiliser d'autres moyens techniques correctement sécurisés pour échanger des informations supplémentaires.

2. Ces informations sont utilisées uniquement aux fins auxquelles elles ont été transmises.

3. Les États membres répondent dans les meilleurs délais aux demandes d'informations supplémentaires adressées par les autres États membres.

4. Les modalités relatives à l'échange d'informations supplémentaires sont adoptées conformément à la procédure visée à l'article 67, sous la forme du «manuel Sirene», sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

Article 9

Conformité technique

1. Afin de permettre une transmission rapide et efficace des données, chaque État membre applique, lors de la création de son N.SIS II, les protocoles et les procédures techniques établis afin de permettre la compatibilité de son N.SIS II avec le CS-SIS. Ces protocoles et ces procédures techniques sont établis conformément à la procédure visée à l'article 67, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

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

Article 10

Sécurité — États membres

1. Chaque État membre adopte, pour son N.SIS II, les mesures, y compris un plan de sécurité, propres à:

a) protéger physiquement les données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques;

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

c) empêcher que des supports de données puissent être lus, copiés, modifiés ou éloignés par une personne non autorisée (contrôle des supports de données);

d) empêcher l'introduction non autorisée dans le fichier, ainsi que toute consultation, toute modification ou tout effacement non autorisés de données à caractère personnel intégrées (contrôle du stockage);

e) empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);

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

g) garantir que toutes les autorités ayant un droit d'accès au SIS II ou aux installations de traitement de données créent des profils décrivant les tâches et responsabilités qui incombent aux personnes habilités en matière d'accès, d'introduction, de mise à jour, de suppression et de consultation des données et mettent sans tarder et à leur demande ces profils à la disposition des autorités de contrôle nationales visées à l'article 60 (profils des membres du personnel);

h) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises par des installations de transmission de données (contrôle de la transmission);

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

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

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

2. Les États membres prennent des mesures équivalentes à celles visées au paragraphe 1, en matière de sécurité des échanges d'informations supplémentaires.

Article 11

Confidentialité — États membres

Chaque État membre applique à l'égard de toutes les personnes et instances appelées à travailler avec des données et des informations supplémentaires du SIS II ses règles relatives au secret professionnel ou à toute obligation de confidentialité équivalente, 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 instances ont cessé leur activité.

Article 12

Conservation des enregistrements au niveau national

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

2. Les États membres qui utilisent des copies nationales veillent à ce que tout accès aux données du SIS II et tout échange de ces données soient enregistrés aux fins mentionnées au paragraphe 1. Ceci n'est pas applicable aux traitements visés à l'article 4, paragraphe 4.

3. Les enregistrements indiquent, en particulier, l'historique des signalements, la date et l'heure de la transmission des données, les données utilisées pour effectuer une consultation, la référence des données transmises et le nom de l'autorité compétente et de la personne responsable du traitement des données.

4. Les enregistrements ne peuvent être utilisés qu'aux fins prévues aux paragraphes 1 et 2 et sont effacés au plus tôt après un an et au plus tard trois ans après leur création. Les enregistrements contenant l'historique des signalements sont effacés après un à trois ans suivant la suppression des signalements.

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

6. Les autorités nationales compétentes chargées de contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS II, ainsi que l'intégrité et la sécurité des données, ont accès, dans les limites de leurs compétences et sur demande, à ces enregistrements 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 II prenne les mesures nécessaires pour se conformer à la présente décision et coopèrent, le cas échéant, avec l'autorité de contrôle nationale.

Article 14

Formation du personnel

Avant d'être autorisé à traiter des données stockées dans le SIS II, le personnel des autorités ayant un droit d'accès au SIS II reçoit une formation appropriée concernant les règles en matière de sécurité et de protection des données et est informé des infractions et des sanctions pénales éventuelles en la matière.

CHAPITRE III

RESPONSABILITÉS INCOMBANT À L'INSTANCE GESTIONNAIRE

Article 15

Gestion opérationnelle

1. Après une période transitoire, une instance gestionnaire, dont le financement est assuré par le budget général de l'Union européenne, est chargée de la gestion opérationnelle du SIS II central. L'instance gestionnaire veille, en collaboration avec les États membres, à ce que le SIS II central utilise en permanence la meilleure technologie disponible, sous réserve d'une analyse coûts/avantages.

2. Il incombe aussi à l'instance gestionnaire d'assurer les tâches ci-après, liées à l'infrastructure de communication:

a) supervision;

b) sécurité;

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

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

a) tâches relatives à la mise en œuvre du budget;

b) acquisition et renouvellement;

c) questions contractuelles.

4. Au cours d'une période transitoire avant que l'instance gestionnaire n'assume ses responsabilités, la Commission est chargée de la gestion opérationnelle du SIS II central. Conformément au règlement (CE, Euratom) n° 1605/2002 du Conseil du 25 juin 2002 portant règlement financier applicable au budget général des Communautés européennes [1], la Commission peut déléguer cette tâche et les tâches de mise en œuvre du budget à des organismes publics nationaux, dans deux pays différents.

5. Chacun des organismes publics nationaux visés au paragraphe 4 doit satisfaire en particulier aux critères de sélection suivants:

a) justifier d'une expérience de longue date acquise dans la gestion d'un système d'information à grande échelle ayant les fonctionnalités visées à l'article 4, paragraphe 4;

b) posséder un savoir-faire remarquable en ce qui concerne les exigences de fonctionnement et de sécurité d'un système d'information ayant des fonctionnalités comparables à celles visées à l'article 4, paragraphe 4;

c) disposer d'un personnel suffisant et expérimenté ayant les qualifications professionnelles et linguistiques requises pour travailler dans un environnement de coopération internationale tel que celui qui est requis par le SIS II;

d) disposer d'infrastructures sécurisées et adaptées à ses besoins, qui soient notamment en mesure de prendre le relais de systèmes TI à grande échelle et d'en assurer le fonctionnement continu; et

e) œuvrer dans un contexte administratif qui lui permette de s'acquitter adéquatement de ses tâches et d'éviter tout conflit d'intérêts.

6. Avant toute délégation telle que visée au paragraphe 4, et à intervalles réguliers par la suite, la Commission informe le Parlement européen et le Conseil des conditions de la délégation, de son champ d'application et des organismes auxquels des tâches sont déléguées.

7. Dans le cas où, conformément au paragraphe 4, la Commission délègue sa responsabilité au cours de la période transitoire, elle veille à ce que cette délégation respecte pleinement les limites fixées par le système institutionnel énoncé dans le traité. Elle veille, en particulier, à ce que cette délégation ne porte pas préjudice à tout mécanisme permettant un contrôle effectif exercé, en vertu du droit communautaire, par la Cour de justice, la Cour des comptes ou le Contrôleur européen de la protection des données.

8. La gestion opérationnelle du SIS II central comprend toutes les tâches nécessaires pour que 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.

[1] JO L 248 du 16.9.2002, p. 1.

Article 16

Sécurité

1. L'instance gestionnaire et la Commission adoptent, respectivement pour le SIS II central et l'infrastructure de communication, les mesures, y compris un plan de sécurité, propres à:

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

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

c) empêcher la lecture, la reproduction, la modification ou l'extraction des supports de données par une personne non autorisée (contrôle des supports de données);

d) empêcher l'introduction non autorisée de données dans le fichier ainsi que toute inspection, modification ou effacement non autorisés de données à caractère personnel enregistrées (contrôle du stockage);

e) empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);

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

g) créer des profils décrivant les tâches et responsabilités qui incombent aux personnes habilités en matière d'accès aux données ou aux installations de traitement de données et à mettre sans tarder et à sa demande ces profils à la disposition du Contrôleur européen de la protection des données visée à l'article 61 (profils des membres du personnel);

h) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises par des installations de transmission de données (contrôle de la transmission);

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

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

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

2. L'instance gestionnaire prend des mesures équivalentes à celles visées au paragraphe 1 concernant la sécurité de l'échange d'informations supplémentaires par le biais de l'infrastructure de communication.

Article 17

Confidentialité — Instance gestionnaire

1. Sans préjudice de l'article 17 du statut des fonctionnaires des Communautés européennes, l'instance gestionnaire applique des règles appropriées en matière de secret professionnel, ou impose des obligations de confidentialité équivalentes, qui s'appliquent à tous les membres de son personnel appelés à travailler avec des données du SIS II et répondent à des normes comparables à celles visées à l'article 11 de la présente décision. 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'instance gestionnaire prend des mesures équivalentes à celles visées au paragraphe 1 pour assurer la confidentialité de l'échange d'informations supplémentaires par le biais de l'infrastructure de communication.

Article 18

Tenue d'enregistrements au niveau central

1. L'instance gestionnaire veille à ce que tous les accès aux données à caractère personnel et tous les échanges de telles données tenues dans le CS-SIS soient enregistrés aux fins mentionnées à l'article 12, paragraphes 1 et 2.

2. Les enregistrements indiquent, en particulier, l'historique des signalements, la date et l'heure de la transmission des données, les données utilisées pour effectuer des consultations, la référence des données transmises et l'identification de l'autorité compétente responsable du traitement des données.

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

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

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

Article 19

Campagne d'information

La Commission, en coopération avec les autorités de contrôle nationales et le Contrôleur européen de la protection des données, accompagne la mise en service du SIS II d'une campagne d'information visant à faire connaître au public les objectifs, les données stockées, les autorités disposant d'un droit d'accès aux signalements et les droits des personnes. Après sa mise en place, l'instance gestionnaire, en coopération avec les autorités de contrôle nationales et le Contrôleur européen de la protection des données, mène régulièrement des campagnes de ce type. Les États membres, en coopération avec leurs autorités de contrôle nationales, élaborent et mettent en œuvre les politiques nécessaires pour informer de manière générale leurs citoyens sur le SIS II.

CHAPITRE IV

CATÉGORIES DE DONNÉES ET APPOSITION D'UN INDICATEUR DE VALIDITÉ

Article 20

Catégories de données

1. Sans préjudice des dispositions de l'article 8, paragraphe 1, ou des dispositions de la présente décision prévoyant le stockage de données complémentaires, le SIS II comporte exclusivement les catégories de données qui sont fournies par chacun des États membres et qui sont nécessaires aux fins prévues aux articles 26, 32, 36, et 38.

2. Les catégories de données sont les suivantes:

a) les personnes signalées;

b) les objets visés aux articles 36 et 38.

3. Les renseignements concernant les personnes signalées comprennent au maximum les éléments suivants:

a) les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, éventuellement enregistrés séparément;

b) les signes physiques particuliers, objectifs et inaltérables;

c) le lieu et la date de naissance;

d) le sexe;

e) les photographies;

f) les empreintes digitales;

g) la ou les nationalités;

h) l'indication que la personne concernée est armée, violente ou en fuite;

i) le motif du signalement;

j) l'autorité signalante;

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

l) les mesures à prendre;

m) le(s) lien(s) vers d'autres signalements introduits dans le SIS II conformément à l'article 52;

n) le type d'infraction.

4. Les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées aux paragraphes 2 et 3, sont établies conformément à la procédure définie à l'article 67, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

5. Les règles techniques nécessaires pour la consultation des données visées au paragraphe 3 sont analogues à celles des consultations dans le CS-SIS, dans les copies nationales et dans les copies techniques, conformément à l'article 46, paragraphe 2.

Article 21

Proportionnalité

Avant d'introduire un signalement, l'État membre signalant vérifie si le cas est suffisamment approprié, pertinent et important pour justifier l'introduction du signalement dans le SIS II.

Article 22

Règles particulières concernant les photographies et les empreintes digitales

L'utilisation des photographies et les empreintes digitales visées à l'article 20, paragraphe 3, points e) et f), est soumise aux dispositions suivantes:

a) les photographies et les empreintes digitales ne sont introduites qu'après avoir été soumises à un contrôle de qualité spécifique visant à garantir le respect de normes minimales en matière de qualité. Les caractéristiques de ce contrôle de qualité spécifique sont fixées conformément à la procédure visée à l'article 67, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire;

b) les photographies et les empreintes digitales ne sont utilisées que pour confirmer l'identité d'une personne trouvée à la suite d'une consultation alphanumérique effectuée dans le SIS II;

c) dès que cela est possible d'un point de vue technique, les empreintes digitales peuvent aussi être utilisées pour identifier une personne sur la base de ses identificateurs biométriques. Avant que cette fonctionnalité soit introduite dans le SIS II, la Commission présente un rapport précisant si la technique requise est disponible et prête à être employée; le Parlement européen est consulté.

Article 23

Exigence à remplir pour l'introduction d'un signalement

1. Les signalements ne peuvent être introduits sans les données visées à l'article 20, paragraphe 3, points a), d) et l) ainsi que, le cas échéant, le point k).

2. En outre lorsqu'elles sont disponibles, toutes les autres données énumérées à l'article 20, paragraphe 3, sont aussi introduites.

Article 24

Dispositions générales concernant l'apposition d'un indicateur de validité

1. Si un État membre estime que la mise en œuvre d'un signalement introduit conformément aux articles 26, 32 ou 36 n'est pas compatible avec son droit national, ses obligations internationales ou des intérêts nationaux essentiels, il peut exiger par la suite que soit apposé sur ledit signalement un indicateur de validité visant à ce que l'exécution de la conduite à tenir en raison de ce signalement n'ait pas lieu sur son territoire. L'indicateur de validité est apposé par le bureau Sirene de l'État membre qui a introduit le signalement.

2. Afin de permettre à un État membre de demander qu'un indicateur de validité soit apposé sur un signalement effectué conformément à l'article 26, tous les États membres sont informés automatiquement, par l'échange d'informations supplémentaires, de tout nouveau signalement relevant de cette catégorie.

3. Si, dans des cas particulièrement urgents et graves, un État membre signalant demande l'exécution de la conduite à tenir, l'État membre d'exécution examine s'il peut autoriser le retrait de l'indicateur de validité qui a été apposé à sa demande. Si l'État membre d'exécution est en mesure de le faire, il prend les dispositions nécessaires afin que la conduite à tenir puisse être exécutée sans délai.

Article 25

Apposition d'un indicateur de validité sur les signalements en vue d'une arrestation aux fins de remise

1. Lorsque la décision-cadre 2002/584/JAI s'applique, l'indicateur de validité visant à prévenir une arrestation ne peut être apposé sur un signalement en vue d'arrestation aux fins de remise que si l'autorité judiciaire compétente en vertu de la législation nationale pour l'exécution d'un mandat d'arrêt européen a refusé cette exécution en invoquant un motif de non-exécution et que l'apposition de l'indicateur de validité a été demandée.

2. Toutefois, à la demande d'une autorité judiciaire compétente en vertu de la législation nationale, l'apposition d'un indicateur de validité à un signalement en vue d'une arrestation aux fins de remise peut également être demandée si, sur la base d'une instruction générale ou dans un cas particulier, il est évident que l'exécution du mandat d'arrêt européen devra être refusée.

CHAPITRE V

SIGNALEMENTS CONCERNANT DES PERSONNES RECHERCHÉES EN VUE D'UNE ARRESTATION AUX FINS DE REMISE OU D'EXTRADITION

Article 26

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données relatives aux personnes recherchées en vue d'une arrestation aux fins de remise sur la base d'un mandat d'arrêt européen ou recherchées en vue d'une arrestation aux fins d'extradition sont introduites à la demande de l'autorité judiciaire de l'État membre signalant.

2. Les données relatives aux personnes recherchées en vue d'une arrestation aux fins de remise sont également introduites sur la base des mandats d'arrêt émis conformément aux accords conclus entre l'Union européenne et des pays tiers sur la base des articles 24 et 38 du traité UE, aux fins de remise de personnes sur la base d'un mandat d'arrêt, qui prévoient la transmission d'un tel mandat d'arrêt par le biais du système d'information Schengen.

Article 27

Données complémentaires concernant les personnes recherchées en vue d'une arrestation aux fins de remise

1. Si une personne est recherchée en vue d'une arrestation aux fins de remise sur la base d'un mandat d'arrêt européen, l'État membre signalant introduit dans le SIS II une copie de l'original du mandat d'arrêt européen.

2. L'État membre signalant peut ajouter une copie de la traduction du mandat d'arrêt européen dans une ou plusieurs autres langues officielles de l'Union européenne

Article 28

Informations supplémentaires concernant les personnes recherchées en vue d'une arrestation aux fins de remise

L'État membre qui a introduit le signalement dans le SIS II en vue d'une arrestation aux fins de remise communique à tous les États membres les informations visées à l'article 8, paragraphe 1, de la décision cadre 2002/584/JAI par le biais de l'échange d'informations supplémentaires.

Article 29

Informations supplémentaires concernant les personnes recherchées en vue d'une arrestation aux fins d'extradition

1. L'État membre qui a introduit le signalement dans le SIS II en vue d'une extradition communique à tous les États membres les données ci-après par le biais de l'échange d'informations supplémentaires:

a) l'autorité dont émane la demande d'arrestation;

b) l'existence d'un mandat d'arrêt ou d'un acte ayant la même force, ou d'un jugement exécutoire;

c) la nature et la qualification légale de l'infraction;

d) la description des circonstances de la commission de l'infraction, y compris le moment, le lieu et le degré de participation à l'infraction de la personne signalée;

e) dans la mesure du possible, les conséquences de l'infraction;

f) toute autre information utile ou nécessaire à l'exécution du signalement.

2. Les données mentionnées au paragraphe 1 ne sont pas communiquées lorsque les données visées aux articles 27 ou 28 ont déjà été fournies et sont considérées comme suffisantes pour l'exécution du signalement par l'État membre concerné.

Article 30

Conversion des signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition

S'il n'est pas possible de procéder à une arrestation soit en raison d'une décision de refus prise par un État membre requis conformément aux procédures relatives à l'apposition d'un indicateur de validité prévues aux articles 24 et 25, soit parce que, dans le cas d'un signalement en vue d'une arrestation aux fins d'extradition, une enquête n'est pas encore terminée, l'État membre requis doit traiter le signalement comme étant un signalement aux fins de communication du lieu où se trouve la personne concernée.

Article 31

Exécution de la conduite à tenir demandée dans le signalement concernant une personne recherchée en vue d'une arrestation aux fins de remise ou d'extradition

1. Un signalement introduit dans le SIS II conformément à l'article 26, associé aux données complémentaires visées à l'article 27, constitue et produit les mêmes effets qu'un mandat d'arrêt européen émis conformément à la décision-cadre 2002/584/JAI, lorsque celle-ci s'applique.

2. Lorsque la décision-cadre 2002/584/JAI ne s'applique pas, un signalement introduit dans le SIS II conformément aux articles 26 et 29 a le même effet légal qu'une demande d'arrestation provisoire au sens de l'article 16 de la convention européenne d'extradition du 13 décembre 1957 ou de l'article 15 du traité Benelux d'extradition et d'entraide judiciaire en matière pénale du 27 juin 1962.

CHAPITRE VI

SIGNALEMENTS CONCERNANT DES PERSONNES DISPARUES

Article 32

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données relatives aux personnes disparues qui doivent être placées sous protection et/ou dont il convient d'établir la localisation sont introduites dans le SIS II à la demande de l'autorité compétente de l'État membre signalant.

2. Les catégories ci-après de personnes disparues peuvent être introduites:

a) les personnes disparues devant être placées sous protection:

   i) dans l'intérêt de leur propre protection;

   ii) pour la prévention de menaces; et

b) les personnes disparues ne devant pas être placées sous protection.

3. Le paragraphe 2, point a), s'applique uniquement aux personnes qui doivent être internées sur décision d'une autorité compétente.

4. Les paragraphes 1, 2 et 3 s'appliquent particulièrement aux mineurs.

5. Les États membres veillent à ce que les données introduites dans le SIS II précisent à quelle catégories mentionnées au paragraphe 2 appartient la personne disparue.

Article 33

Exécution de la conduite à tenir demandée dans un signalement

1. Lorsqu'une personne visée à l'article 32 est retrouvée, les autorités compétentes communiquent le lieu où elle se trouve à l'État membre signalant, sous réserve des dispositions du paragraphe 2. Ces autorités peuvent, dans les cas visés à l'article 32, paragraphe 2, point a), placer les personnes concernées en sécurité aux fins de les empêcher de poursuivre leur voyage, si la législation nationale l'autorise.

2. La communication de données, autre que celle qui a lieu entre les autorités compétentes, concernant une personne majeure disparue qui a été retrouvée est subordonnée au consentement de cette personne. Cependant, les autorités compétentes peuvent indiquer que le signalement a été effacé, du fait que la personne a été localisée, à une personne intéressée qui a signalé la disparition.

CHAPITRE VII

SIGNALEMENTS CONCERNANT DES PERSONNES RECHERCHÉES DANS LE BUT DE RENDRE POSSIBLE LEUR CONCOURS DANS LE CADRE D'UNE PROCÉDURE JUDICIAIRE

Article 34

Objectifs des signalements et conditions auxquelles ils sont soumis

Aux fins de la communication du lieu de séjour ou du domicile, les États membres introduisent dans le SIS II, à la demande d'une autorité compétente, des données relatives:

a) aux témoins;

b) aux personnes citées à comparaître ou recherchées pour être citées à comparaître devant les autorités judiciaires dans le cadre d'une procédure pénale afin de répondre de faits pour lesquels elles font l'objet de poursuites;

c) aux personnes qui doivent faire l'objet d'une notification d'un jugement répressif ou d'autres documents en rapport avec une procédure pénale afin de répondre de faits pour lesquels elles font l'objet de poursuites;

d) aux personnes qui doivent faire l'objet d'une demande de se présenter pour subir une peine privative de liberté.

Article 35

Exécution de la conduite à tenir demandée dans un signalement

Les renseignements demandés sont communiqués à l'État membre requérant par voie d'échange d'informations supplémentaires.

CHAPITRE VIII

SIGNALEMENTS CONCERNANT DES PERSONNES OU DES OBJETS AUX FINS DE CONTRÔLE DISCRET OU DE CONTRÔLE SPÉCIFIQUE

Article 36

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données concernant des personnes ou des véhicules, des embarcations, des aéronefs ou des conteneurs sont introduites conformément au droit national de l'État membre signalant, aux fins de contrôle discret et de contrôle spécifique, conformément à l'article 37, paragraphe 4.

2. Un tel signalement peut être effectué pour la répression d'infractions pénales et pour la prévention de menaces pour la sécurité publique:

a) lorsqu'il existe des indices réels laissant supposer qu'une personne a l'intention de commettre ou commet une infraction pénale grave, telle qu'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI; ou

b) lorsque l'appréciation globale portée sur une personne, en particulier sur la base des infractions pénales commises jusqu'alors, laisse supposer qu'elle commettra également à l'avenir des infractions pénales graves, telles que les infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/548/JAI.

3. En outre, le signalement peut être effectué conformément au droit national, à la demande des instances compétentes pour la sûreté de l'État, lorsque des indices concrets laissent supposer que les informations visées à l'article 37, paragraphe 1, sont nécessaires à la prévention d'une menace grave émanant de l'intéressé ou d'autres menaces graves pour la sûreté intérieure et extérieure de l'État. L'État membre procédant au signalement en vertu du présent paragraphe en tient informés les autres États membres. Chaque État membre détermine à quelles autorités cette information est transmise.

4. Des signalements relatifs aux véhicules, aux embarcations, aux aéronefs ou aux conteneurs peuvent être introduits lorsqu'il existe des indices réels de l'existence d'un lien entre ceux-ci et des infractions pénales graves visées au paragraphe 2 ou des menaces graves visées au paragraphe 3.

Article 37

Exécution de la conduite à tenir demandée dans un signalement

1. Dans le cadre des contrôles discrets ou des contrôles spécifiques, les informations ci-après peuvent, en tout ou en partie, être recueillies et transmises à l'autorité signalante, à l'occasion de contrôles aux frontières ou d'autres contrôles de police et des douanes exercés à l'intérieur du pays:

a) le fait que la personne signalée ou le véhicule, l'embarcation, l'aéronef ou le conteneur signalé a été retrouvé;

b) le lieu, la date et l'heure ou le motif du contrôle;

c) l'itinéraire suivi et la destination visée;

d) les personnes qui accompagnent les intéressés ou les occupants du véhicule, de l'embarcation ou de l'aéronef dont il est permis de supposer qu'ils sont associés aux intéressés;

e) le véhicule, l'embarcation, l'aéronef ou le conteneur utilisé;

f) les objets transportés;

g) les circonstances dans lesquelles la personne ou le véhicule, l'embarcation, l'aéronef ou le conteneur a été retrouvé.

2. Les informations visées au paragraphe 1 sont communiquées grâce à l'échange d'informations supplémentaires.

3. Dans le cadre de la collecte des informations visées au paragraphe 1, les États membres prennent les mesures nécessaires pour ne pas mettre en péril le caractère discret du contrôle.

4. Pendant les contrôles discrets, les personnes, les véhicules, les embarcations, les aéronefs, les conteneurs et les objets transportés peuvent être fouillés conformément au droit national, aux fins visées à l'article 36. Si le contrôle spécifique n'est pas autorisé selon la loi d'un État membre, il se trouve automatiquement converti, dans cet État membre, en contrôle discret.

CHAPITRE IX

SIGNALEMENTS CONCERNANT DES OBJETS AUX FINS D'UNE SAISIE OU DE LA PREUVE DANS UNE PROCÉDURE PÉNALE

Article 38

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données relatives aux objets recherchés aux fins d'une saisie ou de la preuve dans une procédure pénale sont intégrées dans le SIS II.

2. Les catégories ci-après d'objets facilement identifiables sont introduites:

a) les véhicules à moteur d'une cylindrée supérieure à 50 cm^3, les embarcations et les aéronefs;

b) les remorques d'un poids à vide supérieur à 750 kg, les caravanes, le matériel industriel, les moteurs hors-bord et les conteneurs;

c) les armes à feu;

d) les documents officiels vierges volés, détournés ou égarés;

e) les documents d'identité tels que passeports, cartes d'identité, permis de conduire, titres de séjour et documents de voyage délivrés qui ont été volés, détournés, égarés ou invalidés;

f) les certificats d'immatriculation et les plaques d'immatriculation volés, détournés, égarés ou invalidés;

g) les billets de banque (billets enregistrés);

h) les titres et les moyens de paiement tels que chèques, cartes de crédit, obligations et actions volés, détournés, égarés ou invalidés.

3. Les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées au paragraphe 2 sont établies conformément à la procédure visée à l'article 67, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

Article 39

Exécution de la conduite à tenir demandée dans un signalement

1. Si une interrogation fait apparaître l'existence d'un signalement pour un objet trouvé, l'autorité qui l'a constaté se met en rapport avec l'autorité signalante afin de convenir des mesures nécessaires. À cette fin, des données à caractère personnel peuvent également être transmises conformément à la présente décision.

2. Les informations visées au paragraphe 1 sont communiquées grâce à l'échange d'informations supplémentaires.

3. L'État membre qui a trouvé l'objet prend les mesures conformément à son droit national.

CHAPITRE X

DROIT D'ACCÈS ET CONSERVATION DES SIGNALEMENTS

Article 40

Autorités disposant d'un droit d'accès aux signalements

1. L'accès aux données introduites dans le SIS II ainsi que le droit de les interroger directement ou d'interroger une copie des données du SIS II sont réservés exclusivement aux instances qui sont compétentes pour:

a) les contrôles aux frontières, conformément au règlement (CE) n° 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) [1];

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

2. Toutefois, le droit d'accès aux données introduites dans le SIS II et le droit de les consulter directement peuvent également être exercés par les autorités judiciaires nationales, y compris celles qui sont compétentes pour engager des poursuites judiciaires dans le cadre de procédures pénales et des enquêtes judiciaires avant l'inculpation, dans l'exercice de leurs fonctions telles que les définit la législation nationale, et par leurs autorités de coordination.

[1] JO L 105 du 13.4.2006, p. 1.

3. Les autorités visées au présent article sont incluses dans la liste prévue à l'article 46, paragraphe 8.

Article 41

Accès d'Europol aux données du SIS II

1. L'Office européen de police (Europol) a le droit, dans les limites de son mandat, d'accéder aux données introduites dans le SIS II conformément aux articles 26, 36 et 38 et de les consulter directement.

2. Lorsqu'il ressort d'une consultation du système par Europol qu'il existe un signalement dans le SIS II, Europol en informe l'État membre dont émane le signalement par le biais des canaux définis dans la convention Europol.

3. L'utilisation des informations obtenues lors de la consultation du SIS II est soumise à l'accord de l'État membre concerné. Si ledit État membre autorise l'utilisation de ces informations, leur traitement est régi par la convention Europol. Europol ne peut communiquer ces informations à des pays ou instances tiers qu'avec le consentement de l'État concerné.

4. Europol peut demander d'autres informations aux États membres concernés, conformément aux dispositions de la convention Europol.

5. Europol doit:

a) enregistrer chaque accès aux données et chaque recherche qu'il a effectuée, conformément aux dispositions de l'article 12;

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

c) limiter l'accès aux données introduites dans le SIS II au personnel dûment autorisé d'Europol;

d) adopter et appliquer les mesures prévues à l'article 10 et à l'article 11;

e) autoriser l'autorité de contrôle commune, créée en vertu de l'article 24 de la convention Europol, à contrôler les activités d'Europol dans l'exercice de son droit d'accès aux données introduites dans le SIS II et de consultation desdites données.

Article 42

Accès d'Eurojust aux données du SIS II

1. Les membres nationaux d'Eurojust, ainsi que leurs assistants, ont le droit, dans les limites de leur mandat, d'accéder aux données introduites dans le SIS II conformément aux articles 26, 32, 34 et 38 et de les consulter.

2. Lorsqu'il ressort d'une consultation du système par un membre national d'Eurojust qu'il existe un signalement dans le SIS II, celui-ci en informe l'État membre dont émane le signalement. Les informations obtenues lors d'une telle consultation ne peuvent être communiquées à des pays ou instances tiers qu'avec le consentement de l'État dont émane le signalement.

3. Aucune disposition du présent article ne doit être interprétée comme affectant les dispositions de la décision 2002/187/JAI relatives à la protection des données et à la responsabilité du fait d'un traitement non autorisé ou incorrect de données par les membres nationaux d'Eurojust ou leurs assistants, ni comme affectant les prérogatives de l'organe de contrôle commun institué conformément à ladite décision.

4. Chaque accès aux données et chaque recherche effectuée par un membre national d'Eurojust ou un assistant est enregistré conformément aux dispositions de l'article 12 et toute utilisation qu'ils ont faite des données auxquelles ils ont eu accès est enregistrée.

5. Aucune des parties du SIS II auxquelles les membres nationaux ou leurs assistants ont accès ne doit être connectée à un système informatique destiné à la collecte et au traitement des données exploité par Eurojust ou en son sein, et aucune des données contenues dans les premières ne doit être transférée vers le second, ni aucune partie du SIS II téléchargée.

6. L'accès aux données introduites dans le SIS II est limité aux membres nationaux et à leurs assistants et ne s'étend pas au personnel d'Eurojust.

7. Les mesures visant à garantir la sécurité et la confidentialité prévues à l'article 10 et à l'article 11 sont adoptées et appliquées.

Article 43

Limites d'accès

Les utilisateurs, y compris Europol, les membres nationaux d'Eurojust, ainsi que leurs assistants, ne peuvent accéder qu'aux données qui sont nécessaires à l'accomplissement de leurs missions.

Article 44

Durée de conservation des signalements concernant des personnes

1. Les signalements concernant des personnes introduits dans le SIS II en vertu de la présente décision ne sont conservés que pendant le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits.

2. Dans les trois ans à compter de l'introduction d'un tel signalement dans le SIS II, l'État membre signalant examine la nécessité de l'y maintenir. Ce délai est d'un an pour les signalements concernant des personnes visés à l'article 36.

3. Chaque État membre fixe, le cas échéant, des délais d'examen plus courts, conformément à son droit national.

4. L'État membre signalant peut, dans le délai d'examen, décider, au terme d'une évaluation individuelle globale, qui est enregistrée, de maintenir le signalement si ce maintien est nécessaire aux fins qui sont à la base du signalement. Dans ce cas, le paragraphe 2 s'applique également à la prolongation. Toute prolongation du signalement doit être communiquée au CS-SIS.

5. Les signalements sont automatiquement effacés à l'expiration du délai d'examen visé au paragraphe 2, sauf dans le cas où l'État membre signalant a communiqué la prolongation du signalement conformément au paragraphe 4. Le CS-SIS signale automatiquement aux États membres l'effacement programmé des données dans le système avec un préavis de quatre mois.

6. Les États membres tiennent des statistiques concernant le nombre de signalements dont la durée de conservation est prolongée conformément au paragraphe 4.

Article 45

Durée de conservation des signalements concernant des objets

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

2. Les signalements concernant des objets, introduits conformément à l'article 36, sont conservés pendant une durée maximale de cinq ans.

3. Les signalements concernant des objets, introduits conformément à l'article 38, sont conservés pendant une durée maximale de dix ans.

4. Les délais de conservation visés aux paragraphes 2 et 3 peuvent être prolongés si les fins auxquelles le signalement a été effectué l'exigent. Dans ce cas, les paragraphes 2 et 3 s'appliquent également à la prolongation.

CHAPITRE XI

RÈGLES GÉNÉRALES RELATIVES AU TRAITEMENT DES DONNÉES

Article 46

Traitement des données du SIS II

1. Les États membres ne peuvent traiter les données prévues aux articles 20, 26, 32, 34, 36 et 38 qu'aux fins énoncées pour chacune des catégories de signalements visée à ces articles.

2. Les données ne peuvent être copiées qu'à des fins techniques, pour autant que cette copie soit nécessaire aux autorités visées à l'article 40 pour effectuer une consultation directe. Les dispositions de la présente décision s'appliquent à ces copies. Les signalements d'un autre État membre ne peuvent être copiés de leur N.SIS II dans d'autres fichiers nationaux de données.

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

Les États membres tiennent à jour un inventaire de ces copies, le mettent à la disposition des autorités de contrôle nationales et veillent à ce que ces copies soient conformes aux dispositions de la présente décision, et notamment celles de l'article 10.

4. L'accès aux données est autorisé uniquement dans les limites des compétences des autorités nationales visées à l'article 40 et réservé au personnel dûment autorisé.

5. Dans le cadre des signalements prévus aux articles 26, 32, 34, 36 et 38 de la présente décision, tout traitement des informations qui y figurent à des fins autres que celles pour lesquelles elles ont été introduites dans le SIS II doit se rapporter à un cas précis et être justifié par la nécessité de prévenir une menace grave imminente pour l'ordre et la sécurité publics, pour des raisons graves de sûreté de l'État ou aux fins de la prévention d'un fait punissable grave. À cet effet, l'autorisation préalable de l'État membre signalant doit être obtenue.

6. Les données ne pourront pas être utilisées à des fins administratives.

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

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

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

Article 47

Données du SIS II et fichiers nationaux

1. L'article 46, paragraphe 2, n'affecte pas le droit qu'a un État membre de conserver dans son fichier national des données du SIS II sur la base desquelles la conduite à tenir a été exécutée sur son territoire. Ces données sont conservées dans les fichiers nationaux pour une durée maximale de trois ans, sauf si des dispositions particulières du droit national prévoient une durée de conservation plus longue.

2. L'article 46, paragraphe 2, n'affecte pas le droit qu'un État membre a de conserver dans ses fichiers nationaux des données contenues dans un signalement particulier qu'il a lui-même introduit dans le SIS II.

Article 48

Information en cas d'inexécution d'un signalement

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

Article 49

Qualité des données traitées dans le cadre du SIS II

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

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

3. Si un État membre autre que l'État membre signalant dispose d'indices faisant présumer qu'une donnée est entachée d'erreur de fait ou a été stockée illégalement, il en informe l'État membre signalant, par voie d'échange d'informations supplémentaires, dans les meilleurs délais et au plus tard dix jours après avoir relevé ces éléments. L'État membre signalant vérifie ce qui lui est communiqué et, le cas échéant, corrige ou efface la donnée sans délai.

4. Si les États membres ne peuvent parvenir à un accord dans un délai de deux mois, l'État membre qui n'est pas à l'origine du signalement soumet la question au Contrôleur européen de la protection des données qui, en coopération avec les autorités de contrôle nationales concernées agit en tant que médiateur.

5. Les États membres échangent des informations supplémentaires lorsqu'une personne se plaint de ne pas être celle visée par un signalement. Lorsqu'il ressort des vérifications qu'il existe effectivement deux personnes différentes, la personne qui s'est plainte est informée des dispositions de l'article 51.

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

Article 50

Différenciation des personnes présentant des caractéristiques similaires

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

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

b) si la vérification fait apparaître que la personne faisant l'objet du nouveau signalement et la personne déjà signalée dans le SIS II sont bien une seule et même personne, le bureau Sirene met en œuvre la procédure concernant les signalements multiples visée à l'article 49, paragraphe 6. Si la vérification révèle qu'il s'agit en réalité de deux personnes différentes, le bureau Sirene valide la demande du deuxième signalement, en ajoutant les éléments nécessaires pour éviter toute erreur d'identification.

Article 51

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

1. Lorsqu'il est possible de confondre la personne effectivement visée par un signalement et une personne dont l'identité a été usurpée, l'État membre à l'origine du signalement 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 que peuvent entraîner des erreurs d'identification.

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

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

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

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

a) les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes éventuellement enregistrés séparément;

b) les signes physiques particuliers, objectifs et inaltérables;

c) le lieu et la date de naissance;

d) le sexe;

e) les photographies;

f) les empreintes digitales;

g) la ou les nationalités;

h) le numéro du ou des documents d'identité et leur date de délivrance.

4. Les règles techniques nécessaires pour l'introduction et le traitement ultérieur des données visées au paragraphe 3 sont établies conformément à la procédure visée à l'article 67, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

5. Les données visées au paragraphe 3 sont effacées en même temps que le signalement correspondant, ou plus tôt si la personne concernée le demande.

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

Article 52

Mise en relation de signalements

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

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

3. La mise en relation ne porte pas atteinte aux droits d'accès prévus par la présente décision. 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 uniquement lorsque cela répond à un besoin opérationnel manifeste.

5. Un État membre peut créer des liens conformément à son droit national pour autant que les principes énoncés dans le présent article soient respectés.

6. 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 ainsi établi soit inaccessible à partir de son territoire national ou pour les autorités relevant de sa juridiction établies en dehors de son territoire.

7. Les règles techniques relatives à la mise en relation de signalements sont adoptées conformément à la procédure définie à l'article 67, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

Article 53

Objet et durée de conservation des informations supplémentaires

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

2. Les données à caractère personnel conservées au sein du bureau Sirene à la suite d'un échange d'informations ne sont conservées que pendant le temps nécessaire à la réalisation des objectifs pour lesquels elles ont été fournies. Elles sont, en tout état de cause, effacées au plus tard un an après que le signalement concernant la personne en question a été supprimé du SIS II.

3. Le paragraphe 2 n'affecte pas le droit qu'a un État membre de conserver dans des fichiers nationaux des données relatives à un signalement particulier que cet État membre a émis ou qui a donné lieu à l'adoption de mesures sur son territoire. Le délai pendant lequel les données peuvent être conservées dans ces fichiers est régi par la législation nationale.

Article 54

Transfert de données à caractère personnel à des tiers

Les données traitées dans le SIS II conformément à la présente décision ne sont pas transférées à un pays tiers ou à des organisations internationales ni mises à leur disposition.

Article 55

Échange avec Interpol de données concernant les passeports volés, détournés, égarés ou invalidés

1. Par dérogation aux dispositions de l'article 54, le numéro, le pays de délivrance et le type des passeports volés, détournés, égarés ou invalidés qui sont introduits dans le SIS II peuvent être échangés avec des membres d'Interpol en établissant une connexion entre le SIS II et la base de données d'Interpol sur les documents de voyage volés ou manquants, à condition qu'un accord soit conclu entre Interpol et l'Union européenne. L'accord prévoit que la transmission de données introduites par un État membre est soumise à l'approbation de cet État membre.

2. L'accord visé au paragraphe 1 prévoit que les données communiquées ne sont accessibles qu'aux membres d'Interpol de pays assurant un niveau de protection adéquat des données à caractère personnel. Avant de conclure un tel accord, le Conseil demande l'avis de la Commission sur le caractère adéquat du niveau de protection des données à caractère personnel et sur le respect des libertés et droits fondamentaux en ce qui concerne le traitement automatisé des données à caractère personnel par Interpol et par les pays qui ont délégué des membres à Interpol.

3. L'accord visé au paragraphe 1 peut également prévoir que les États membres ont accès, au moyen de SIS II, aux informations contenues dans la base de données d'Interpol sur les documents de voyage volés ou manquants, conformément aux dispositions pertinentes de la présente décision qui régissent les signalements concernant les passeports volés, détournés, égarés ou invalidés introduits dans le SIS II.

CHAPITRE XII

PROTECTION DES DONNÉES

Article 56

Traitement des catégories de données sensibles

Le traitement des catégories de données visées à l'article 6 de la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel est interdit.

Article 57

Application de la convention du Conseil de l'Europe pour la protection des données

Les données à caractère personnel traitées en application de la présente décision sont protégées conformément à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à ses modifications ultérieures.

Article 58

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

1. Le droit de toute personne d'accéder aux données la concernant qui sont introduites dans le SIS II conformément au présent règlement s'exerce dans le respect du droit de l'État membre auprès duquel elle le fait valoir.

2. Si le droit national le prévoit, l'autorité de contrôle nationale décide si des informations doivent être communiquées et selon quelles modalités.

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

4. La communication des informations à la personne concernée est refusée si elle peut nuire à l'exécution d'une tâche légale en liaison avec le signalement ou à la protection des droits et libertés d'autrui.

5. Toute personne a le droit de faire rectifier des données la concernant inexactes dans les faits ou de faire effacer des données la concernant stockées illégalement.

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

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

Article 59

Voies de recours

1. Toute personne peut intenter une action devant les juridictions ou l'autorité compétentes en vertu du droit national de tout État membre, pour accéder, faire rectifier ou effacer des données ou pour obtenir des informations ou une indemnisation en raison d'un signalement la concernant.

2. Les États membres s'engagent mutuellement à exécuter les décisions définitives prises par les juridictions ou autorités visées au paragraphe 1, sans préjudice des dispositions de l'article 64.

3. Les modalités de recours prévues dans le présent article sont évaluées par la Commission au plus tard le 23 août 2009.

Article 60

Contrôle du N.SIS II

1. Chaque État membre veille à ce qu'une autorité indépendante (l'«autorité de contrôle nationale») contrôle en toute indépendance la licéité du traitement des données à caractère personnel dans le cadre du SIS II sur son territoire et leur transmission à partir de celui-ci, y compris pour ce qui concerne l'échange et le traitement ultérieur d'informations supplémentaires.

2. L'autorité de contrôle nationale veille à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données dans le cadre de son N.SIS II, répondant aux normes internationales en matière d'audit.

3. Les États membres veillent à ce que leur autorité de contrôle nationale dispose des ressources nécessaires pour s'acquitter des tâches qui leur sont confiées par la présente décision.

Article 61

Contrôle de l'instance gestionnaire

1. Le Contrôleur européen de la protection des données vérifie que les activités de traitement des données à caractère personnel menées par l'instance gestionnaire sont effectuées conformément au présent règlement. Les fonctions et compétences visées aux articles 46 et 47 du règlement (CE) n° 45/2001 s'appliquent en conséquence.

2. Le Contrôleur européen de la protection des données veille à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données à caractère personnel menées par l'instance gestionnaire conformément aux normes internationales en matière d'audit. Un rapport de cet audit est communiqué au Parlement européen, au Conseil, à l'instance gestionnaire, à la Commission et aux autorités de contrôle nationales. L'instance gestionnaire a la possibilité de formuler des observations avant l'adoption du rapport.

Article 62

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

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

2. Agissant chacun dans le cadre de leurs compétences respectives, ils échangent les informations utiles, s'assistent mutuellement pour mener les audits et inspections, examinent les difficultés d'interprétation ou d'application de la présente décision, étudient les problèmes pouvant se poser lors de l'exercice du contrôle indépendant ou dans l'exercice des droits de la personne concernée, formulent des propositions harmonisées en vue de trouver des solutions communes aux éventuels problèmes et assurent, si nécessaire, la sensibilisation aux droits en matière de protection des données.

3. Les autorités de contrôle nationales et le Contrôleur européen de la protection des données se réunissent à cet effet au minimum deux fois par an. Le coût et l'organisation de ces réunions sont à la charge du Contrôleur 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, si nécessaire. Un rapport d'activités conjoint est transmis tous les deux ans au Parlement européen, au Conseil, à la Commission et à l'instance gestionnaire.

Article 63

Protection des données durant la période transitoire

Au cas où, pendant la période transitoire, la Commission délègue ses responsabilités à une autre instance ou à d'autres instances, conformément à l'article 15, paragraphe 4, elle veille à ce que le Contrôleur européen de la protection des données ait le droit et la possibilité de s'acquitter pleinement de sa mission, y compris de procéder à des vérifications sur place ou d'exercer tout autre pouvoir dont il est investi en vertu de l'article 47 du règlement (CE) nº 45/2001.

CHAPITRE XIII

RESPONSABILITÉ ET SANCTIONS

Article 64

Responsabilité

1. Tout État membre est responsable, conformément à son droit national, de tout dommage causé à une personne du fait de l'exploitation du N.SIS II. Il en est également ainsi lorsque les dommages ont été causés par l'État membre signalant, lorsque celui-ci a introduit des données inexactes dans les faits ou a stocké des données illégalement.

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

3. Si le non-respect, par un État membre, des obligations qui lui incombent en vertu de la présente décision entraîne un dommage pour SIS II, cet État membre en est tenu responsable, sauf si l'instance gestionnaire ou un autre État membre participant au SIS II n'a pas pris de mesures raisonnables pour prévenir le dommage ou pour en atténuer les effets.

Article 65

Sanctions

Les États membres veillent à ce que toute utilisation frauduleuse de données introduites dans le SIS II ou tout échange d'informations supplémentaires contraire à la présente décision fasse l'objet de sanctions effectives, proportionnées et dissuasives conformément à leur droit national.

CHAPITRE XIV

DISPOSITIONS FINALES

Article 66

Contrôle et statistiques

1. L'instance gestionnaire veille à ce que des procédures soient mises en place pour contrôler le fonctionnement du SIS II par rapport aux objectifs fixés, tant en termes de résultats que de rapport coût/efficacité, de sécurité et de qualité de service.

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

3. Chaque année, l'instance gestionnaire publie des statistiques présentant le nombre d'enregistrements par catégorie de signalement, le nombre de résultats positifs par catégorie de signalement et le nombre d'accès au SIS II, sous forme de totaux et ventilées par État membre.

4. Deux ans après la mise en service du SIS II puis tous les deux ans, l'instance gestionnaire présente au Parlement européen et au Conseil un rapport sur le fonctionnement technique du SIS II central et de l'infrastructure de communication, y compris la sécurité qu'elle offre, et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres.

5. Trois ans après la mise en service du SIS II puis tous les quatre ans, la Commission présente un rapport d'évaluation globale du SIS II 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 de la présente décision en ce qui concerne le SIS II central et sur la sécurité offerte par le SIS II central et en tire toutes les conséquences pour le fonctionnement futur. La Commission transmet le rapport d'évaluation au Parlement européen et au Conseil.

6. Les États membres communiquent à l'instance gestionnaire et à la Commission les informations nécessaires pour établir les rapports visés aux paragraphes 3, 4 et 5

7. L'instance gestionnaire fournit à la Commission les informations nécessaires pour élaborer les évaluations globales visées au paragraphe 5.

Article 67

Comité de réglementation

1. Dans le cas où il est fait référence au présent article, la Commission est assistée par un comité de réglementation composé des représentants des États membres et présidé par le représentant de la Commission. Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet dans un délai que le président peut fixer en fonction de l'urgence de la question en cause. L'avis est émis à la majorité prévue à l'article 205, paragraphe 2, du traité CE pour l'adoption des décisions que le Conseil est appelé à prendre sur proposition de la Commission. Lors des votes au sein du comité, les voix des représentants des États membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

2. Le comité adopte son règlement intérieur sur proposition de son président, sur la base d'un règlement intérieur type qui a été publié au *Journal officiel de l'Union européenne*.

3. La Commission arrête les mesures envisagées lorsqu'elles sont conformes à l'avis du comité. Lorsque les mesures envisagées ne sont pas conformes à l'avis du comité, ou en l'absence d'avis, la Commission soumet sans tarder au Conseil une proposition relative aux mesures à prendre.

4. Le Conseil peut statuer à la majorité qualifiée sur la proposition dans un délai de deux mois à compter de la saisine du Conseil. Si, dans ce délai, le Conseil a indiqué, à la majorité qualifiée, qu'il s'oppose à la proposition, la Commission réexamine celle-ci. Elle peut soumettre au Conseil une proposition modifiée, soumettre à nouveau sa proposition ou présenter une proposition législative. Si, à l'expiration de ce délai, le Conseil n'a pas adopté les mesures d'application proposées et n'a pas indiqué qu'il s'opposait à la proposition de mesures d'application, les mesures d'application proposées sont arrêtées par la Commission.

5. Le comité visé au paragraphe 1 exerce ses fonctions à partir de 23 août 2007.

Article 68

Modification des dispositions de l'acquis de Schengen

1. Dans les domaines relevant du traité UE, la présente décision remplace à la date visée à l'article 71, paragraphe 2, les dispositions de l'article 64 et des articles 92 à 119 de la convention de Schengen, à l'exception de son article 102 *bis*.

2. Dans les domaines relevant du traité UE, la présente décision remplace, en outre, à la date visée à l'article 71, paragraphe 2, les dispositions ci-après de l'acquis de Schengen mettant en œuvre lesdits articles [1]:

a) décision du Comité exécutif du 14 décembre 1993 concernant le règlement financier relatif aux frais d'installation et de fonctionnement du système d'information Schengen (C.SIS) [SCH/Com-ex(93) 16];

b) décision du Comité exécutif du 7 octobre 1997 concernant le développement du SIS [SCH/Com-ex (97) 24];

c) décision du Comité exécutif du 15 décembre 1997 concernant la modification du règlement financier relatif au C.SIS [SCH/Com-ex (97) 35];

d) décision du Comité exécutif du 21 avril 1998 concernant le C.SIS avec 15/18 connexions [SCH/Com-ex (98) 11];

e) décision du Comité exécutif du 25 avril 1997 concernant l'adjudication de l'étude préliminaire du SIS II [SCH/Com-ex (97) 2, rév. 2];

f) décision du Comité exécutif du 28 avril 1999 concernant les dépenses d'installation du C.SIS [SCH/Com-ex (99) 4];

g) décision du Comité exécutif du 28 avril 1999 concernant la mise à jour du manuel Sirene [SCH/Com-ex (99) 5];

h) déclaration du Comité exécutif du 18 avril 1996 concernant la définition de la notion d'étranger [SCH/Com-ex (96) décl. 5];

i) déclaration du Comité exécutif du 28 avril 1999 concernant la structure du SIS [SCH/Com-ex (99) décl. 2, rév.];

j) décision du Comité exécutif du 7 octobre 1997 concernant la participation de la Norvège et de l'Islande aux frais d'installation et de fonctionnement du C.SIS [SCH/Com-ex (97) 18].

3. Dans les domaines relevant du traité UE, les références aux articles de la convention de Schengen et aux dispositions pertinentes de l'acquis de Schengen mettant en œuvre ces articles qui sont ainsi remplacés s'entendent comme faites à la présente décision.

Article 69

Abrogation

La décision 2004/201/JAI, la décision 2005/211/JAI, la décision 2005/719/JAI, la décision 2005/727/JAI, la décision 2006/228/JAI, la décision 2006/229/JAI et la décision 2006/631/JAI sont abrogées à la date visée à l'article 71, paragraphe 2.

[1] JO L 239 du 22.9.2000, p. 439.

Article 70

Période transitoire et budget

1. Les signalements sont transférés du SIS 1+ au SIS II. Les États membres veillent, en donnant la priorité aux signalements relatifs aux personnes, à ce que le contenu des signalements qui sont transférés du SIS 1+ au SIS II respecte, dès que possible et dans un délai de trois ans après la date visée à l'article 71, paragraphe 2, les dispositions de la présente décision. Au cours de cette période transitoire, les États membres peuvent continuer d'appliquer les dispositions des articles 94, 95 et 97 à 100 de la convention de Schengen au contenu des signalements qui sont transférés du SIS 1+ au SIS II, à condition de respecter les règles suivantes:

a) au cas où le contenu d'un signalement transféré du SIS 1+ au SIS II ferait l'objet d'une modification, d'un ajout, d'une correction ou d'une mise à jour, les États membres veillent à ce que le signalement respecte les dispositions de la présente décision, à compter de la modification, de l'ajout, de la correction ou de la mise à jour en question;

b) en cas de réponse positive à un signalement transféré du SIS 1+ au SIS II, les États membres examinent immédiatement la compatibilité de ce signalement avec les dispositions de la présente décision, sans retarder les actions à mener sur la base dudit signalement.

2. À la date fixée conformément à l'article 71, paragraphe 2, le reliquat du budget approuvé conformément aux dispositions de l'article 119 de la convention de Schengen est remboursé aux États membres. Les montants à restituer sont calculés sur la base des quote-parts des États membres conformément à la décision du Comité exécutif du 14 décembre 1993 concernant le règlement financier relatif aux frais d'installation et de fonctionnement du système d'information Schengen.

3. Durant la période transitoire prévue à l'article 15, paragraphe 4, dans la présente décision, par instance gestionnaire, on entend la Commission.

Article 71

Entrée en vigueur, applicabilité et passage d'un système à l'autre

1. La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Elle s'applique aux États membres participant au SIS 1+ à compter de dates à arrêter par le Conseil, statuant à l'unanimité de ses membres représentant les gouvernements des États membres participant au SIS 1+.

3. Les dates visées au paragraphe 2 sont arrêtées lorsque:

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

b) tous les États membres participant pleinement au SIS 1+ ont informé la Commission qu'ils avaient pris les dispositions techniques et juridiques nécessaires pour traiter les données du SIS II et échanger des informations supplémentaires;

c) la Commission a déclaré qu'un test complet du SIS II a été effectué de manière concluante, test effectué par la Commission avec les États membres, et lorsque les instances préparatoires du Conseil ont validé les résultats du test proposé et confirmé que le niveau de performance du SIS II est au moins équivalent à celui atteint par le SIS 1+;

d) la Commission a pris les dispositions techniques nécessaires pour permettre la connexion du SIS II central au N.SIS II des États membres concernés.

4. La Commission informe le Parlement européen des résultats des tests effectués conformément au paragraphe 3, point c).

5. Toute décision du Conseil prise conformément au paragraphe 2 est publiée au *Journal officiel de l'Union européenne*.

Fait à Luxembourg, le 12 juin 2007.

Par le Conseil
Le président
W. SCHÄUBLE