►B RÈGLEMENT (CE) Nº 1987/2006 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 20 décembre 2006

sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)

(JO L 381 du 28.12.2006, p. 4)

Modifié par:

		Journal officiel		
		nº	page	date
►M1	Règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018	L 295	99	21.11.2018
►M2	Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018	L 312	14	7.12.2018

Rectifié par:

►C1 Rectificatif, JO L 23 du 29.1.2015, p. 19 (1987/2006)

▼B

RÈGLEMENT (CE) Nº 1987/2006 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 20 décembre 2006

sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Établissement et objectif général du SIS II

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

2. L'objet du SIS II, conformément aux dispositions du présent règlement, 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. Le présent règlement établit les conditions et les procédures relatives à l'introduction et au traitement dans le SIS II des signalements de ressortissants de pays tiers, ainsi qu'à l'échange d'informations supplémentaires et de données complémentaires aux fins de non-admission ou d'interdiction de séjour dans les États membres.

2. Le présent règlement contient également des dispositions concernant l'architecture technique du SIS II et les responsabilités incombant aux États membres et à l'instance gestionnaire visée à l'article 15, des règles générales sur le traitement des données, ainsi que des dispositions sur les droits des personnes concernées et sur la responsabilité.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

a) «signalement», un ensemble de données introduites dans le SIS II permettant aux autorités compétentes d'identifier une personne 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 demandée puisse être exécutée;

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

▼B

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 l'exercice du droit d'accès.

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

d) «ressortissant d'un pays tiers», toute personne qui n'est ni:

i) citoyen de l'Union européenne au sens de l'article 17, paragraphe 1, du traité, ni

ii) ressortissant d'un pays tiers jouissant, en vertu d'accords entre la Communauté et ses États membres, d'une part, et le pays en question, d'autre part, de droits de libre circulation équivalents à ceux des citoyens de l'Union européenne;

e) «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;

f) «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.

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-CIS») contenant la base de données du SIS II;

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

▼B

b) d'un système national (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») comprenant une copie complète ou partielle de la base de données du SIS II;

c) d'une infrastructure de communication entre le CS-SIS et la NI-SIS (l'«infrastructure de communication»), fournissant un réseau virtuel crypté consacré aux données du SIS II et à l'échange 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 concernant le CS-SIS afin d'assurer la fourniture des services visés à l'article 4, paragraphe 4.

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

▼B

CHAPITRE II

RESPONSABILITÉS INCOMBANT AUX ÉTATS MEMBRES

▼M2

Article 6

Systèmes nationaux

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

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

▼B

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 du présent règlement. 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 31, 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.

▼B

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 51, paragraphe 2, 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 51, paragraphe 2, 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);

▼B

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 44, paragraphe 1 (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.

▼M2

Article 11

Confidentialité — États membres

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

▼M2

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

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

▼B

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 aux données à caractère personnel et tout échange de ces données dans le CS-SIS soient enregistrés dans leur 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 N. 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 une période d'un an et au plus tard après une période de trois ans suivant leur création. Les enregistrements contenant l'historique des signalements sont effacés après une période d'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 ou non des consultations, 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.

▼B

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 au présent règlement et coopère, 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.

▼M1

2. L'instance gestionnaire est chargée de l'ensemble des tâches liées à l'infrastructure de communication, en particulier:

a) de la supervision;

b) de la sécurité;

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

d) des tâches relatives à la mise en œuvre du budget;

e) de l'acquisition et du renouvellement; et

f) des questions contractuelles.

▼M2

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

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

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

▼B

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

▼B

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.

▼M2

8. La gestion opérationnelle du SIS II central comprend toutes les tâches nécessaires pour que le SIS II central puisse fonctionner 24 heures sur 24, 7 jours sur 7 conformément au présent règlement, en particulier

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

▼M2

les travaux de maintenance et les développements techniques indispensables au bon fonctionnement du système. Ces tâches incluent également la coordination, la gestion et le soutien des activités de test concernant le SIS II central et les N.SIS II, qui garantissent que le SIS II central et les N.SIS II fonctionnent conformément aux exigences de conformité technique fixées à l'article 9.

▼B

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, mentionné à l'article 45 (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);

▼B

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

j) empêcher, en particulier par des techniques de cryptage adaptées, que, lors de la transmission de données à caractère personnel ou du transport de 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 du présent règlement. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après la fin de leurs activités.

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

▼M2

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

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

▼B

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 au sein du CS-SIS soient enregistrées aux fins mentionnées à l'article 12, paragraphes 1 et 2.

▼B

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

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

Article 20

Catégories de données

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

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

▼B

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;

▼M2

k *bis*) le type d'infraction;

▼B

l) la conduite à tenir;

m) le(s) lien(s) vers d'autres signalements introduits dans le SIS II, conformément à l'article 37.

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 51, paragraphe 2, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

4. Les règles techniques nécessaires pour la consultation des données visées au paragraphe 2 sont analogues à celles des consultations dans le CS-SIS, dans les copies nationales et dans les copies techniques, conformément à l'article 31, 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.

▼M2

Lorsque la décision de non-admission et d'interdiction de séjour visée à l'article 24, paragraphe 2, est liée à une infraction terroriste, le cas est

▼M2

considéré comme étant suffisamment approprié, pertinent et important pour justifier un signalement dans le SIS II. Pour des raisons de sécurité publique ou nationale, les États membres peuvent, à titre exceptionnel, s'abstenir d'introduire un signalement si celui-ci risque de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires.

Article 22

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

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

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

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

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

▼B

Article 23

Exigence à remplir pour l'introduction d'un signalement

1. Un signalement ne peut être introduit sans les données visées à l'article 20, paragraphe 2, points a), d), k) et l).

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

Article 24

Conditions auxquelles sont soumis les signalements introduits aux fins de nonadmission ou d'interdiction de séjour

1. Les données relatives aux ressortissants de pays tiers faisant l'objet d'un signalement aux fins de non-admission ou d'interdiction de séjour sont introduites sur la base d'un signalement national résultant d'une décision prise par les autorités administratives ou juridictions compétentes dans le respect des règles de procédure prévues par la législation nationale, sur la base d'une évaluation individuelle. Les recours contre cette décision sont formés conformément à la législation nationale.

▼B

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

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

b) d'un ressortissant d'un pays tiers à l'égard duquel il existe des raisons sérieuses de croire qu'il a commis un fait punissable grave, ou à l'égard duquel il existe des indices réels qu'il envisage de commettre un tel fait sur le territoire d'un État membre.

3. Un signalement peut également être introduit lorsque la décision visée au paragraphe 1 est fondée sur le fait que le ressortissant d'un pays tiers a fait l'objet d'une mesure d'éloignement, de renvoi ou d'expulsion qui n'a pas été abrogée ni suspendue, et qui comporte ou est assortie d'une interdiction d'entrée, ou, le cas échéant, de séjour, fondée sur le non-respect des réglementations nationales relatives à l'entrée ou au séjour des ressortissants de pays tiers.

4. Le présent article ne s'applique pas aux personnes visées à l'article 26.

5. La Commission réexamine l'application du présent article est trois ans après la date visée à l'article 55, paragraphe 2. Sur la base de ce réexamen, la Commission, utilisant le droit d'initiative que lui confère le traité, fait les propositions nécessaires pour modifier les dispositions du présent article afin de parvenir à un degré plus élevé d'harmonisation des critères de signalement.

Article 25

Conditions auxquelles sont soumis les signalements de ressortissants de pays tiers jouissant du droit de libre circulation dans la Communauté

1. Un signalement concernant un ressortissant de pays tiers qui jouit du droit de libre circulation dans la Communauté au sens de la directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres ([1]), est conforme aux règles adoptées dans le cadre de la mise en œuvre de ladite directive.

2. En cas de réponse positive à un signalement introduit en vertu de l'article 24 qui vise un ressortissant d'un État tiers bénéficiant du droit de libre circulation dans la Communauté, l'État membre d'exécution du signalement consulte immédiatement l'État membre signalant par l'intermédiaire du bureau SIRENE en suivant les dispositions du manuel SIRENE, afin de décider sans délai des mesures à prendre.

([1]) JO L 158 du 30.4.2004, p. 77.

▼M2

Article 26

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

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

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

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

▼B

Article 27

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 consulter directement ou de consulter une copie des données du SIS II sont réservés exclusivement aux autorités qui, en matière d'identification de ressortissants de pays tiers, 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 prévues dans la législation nationale, et par leurs autorités de coordination.

3. En outre, l'accès aux données introduites conformément à l'article 24 et aux données concernant les documents relatifs aux personnes introduites conformément à l'article 38, paragraphe 2, points d) et e), de la ►C1 décision 2007/533/JAI, ◄ ainsi que le droit de les consulter

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

▼B

directement, peuvent être exercés par les autorités qui sont compétentes pour la délivrance des visas, les autorités centrales qui sont compétentes pour l'examen des demandes de visa ainsi que les autorités qui sont compétentes pour la délivrance des titres de séjour et pour la mise en œuvre de la législation sur les ressortissants de pays tiers dans le cadre de l'application des dispositions de l'acquis communautaire relatif à la circulation des personnes. L'accès de ces autorités aux données est régi par le droit national de chaque État membre.

4. Les autorités visées au présent article sont incluses dans la liste prévue à l'article 31, paragraphe 8.

▼M2

Article 27 bis

Accès d'Europol aux données dans le SIS II

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

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

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

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

([1]) Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

▼**M2**

5. Europol:

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

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

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

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

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

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

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

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

▼M2

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

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

Article 27 ter

Accès aux données dans le SIS II par les équipes du corps européen de garde-frontières et de garde-côtes, les équipes d'agents intervenant dans les tâches liées au retour et les membres des équipes d'appui à la gestion des flux migratoires

1. Conformément à l'article 40, paragraphe 8, du règlement (UE) 2016/1624 du Parlement européen et du Conseil ([1]), les membres des équipes visées à l'article 2, points 8) et 9), dudit règlement ont le droit, dans les limites de leur mandat et pour autant que ceux-ci soient autorisés à procéder à des vérifications conformément à l'article 27, paragraphe 1, du présent règlement et qu'ils aient reçu la formation requise conformément à l'article 14 du présent règlement, d'avoir accès aux données dans le SIS II et d'effectuer des recherches dans ces données dans la mesure où cela est nécessaire à l'exécution de leurs missions et où cela est requis par le plan opérationnel pour une opération spécifique. L'accès aux données dans le SIS II ne s'étend pas à d'autres membres des équipes.

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

3. Lorsqu'une recherche effectuée par un membre des équipes visé au paragraphe 1 du présent article révèle l'existence d'un signalement dans le SIS II, l'État membre signalant en est informé. Conformément à l'article 40 du règlement (UE) 2016/1624, les membres des équipes n'agissent en réaction à un signalement dans le SIS II que sur les instructions et, en règle générale, en présence de garde-frontières ou d'agents intervenant dans les tâches liées au retour de l'État membre hôte dans lequel ils opèrent. L'État membre hôte peut autoriser les membres des équipes à agir en son nom.

4. Aux fins de vérifier la licéité du traitement des données, d'assurer un autocontrôle et de garantir la sécurité et l'intégrité des données, l'Agence européenne de garde-frontières et de garde-côtes consigne dans des registres tout accès au SIS II et toute recherche effectuée dans le SIS II conformément aux dispositions de l'article 12.

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

▼M2

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

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

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

8. L'Agence européenne de garde-frontières et de garde-côtes autorise le Contrôleur européen de la protection des données à contrôler et à examiner les activités des équipes visées au présent article dans le cadre de l'exercice de leur droit d'accès aux données dans le SIS II et de leur droit d'effectuer des recherches dans ces données. Cette disposition est sans préjudice des autres dispositions du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([1]).

▼B

Article 28

Limites d'accès

Les utilisateurs ne peuvent accéder qu'aux données qui sont nécessaires à l'accomplissement de leurs missions.

Article 29

Durée de conservation des signalements

1. Les signalements 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. 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 le maintenir.

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.

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

▼B

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 au CS-SIS conformément au paragraphe 4. Le CS-SIS signale automatiquement aux États membres l'effacement programmé 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 a été prolongée conformément au paragraphe 4.

Article 30

Acquisition de la citoyenneté et signalements

Les signalements concernant une personne ayant acquis la citoyenneté d'un État dont les ressortissants jouissent du droit de libre circulation dans la Communauté sont effacés dès que l'État membre signalant apprend ou est informé, en application de l'article 34, ou a connaissance, que la personne concernée a acquis cette citoyenneté.

CHAPITRE V

RÈGLES GÉNÉRALES RELATIVES AU TRAITEMENT DES DONNÉES

Article 31

Traitement des données du SIS II

1. Les États membres peuvent traiter les données visées à l'article 20 aux fins de non-admission ou d'interdiction de séjour sur leur territoire.

2. Les données ne peuvent être copiées qu'à des fins techniques, pour autant que cette copie soit nécessaire aux autorités visées à l'article 27 pour effectuer une consultation directe. Les dispositions du présent règlement s'appliquent à ces copies. Les signalements émis par 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 cette situation d'urgence prenne fin.

Nonobstant l'alinéa 1er, les copies techniques alimentant des bases de données hors ligne destinées aux autorités chargées de délivrer les visas ne seront plus autorisées un an après que l'autorité concernée s'est connectée avec succès à l'infrastructure de communication du Système d'information sur les visas, système à établir dans un règlement à venir, concernant le système d'information sur les visas et l'échange de données entre les États membres sur les visas de court séjour, à l'exception des copies faites pour n'être utilisées que dans des situations d'urgence résultant d'une indisponibilité du réseau de plus de vingt-quatre heures.

Les États membres tiennent à jour un inventaire de ces copies, le mettent à la disposition de leurs autorités de contrôle nationales visées à l'article 44, paragraphe 1, et veillent à ce que ces copies soient conformes aux dispositions du présent règlement, et notamment celles de l'article 10.

▼B

4. L'accès aux données est autorisé uniquement dans les limites des compétences des autorités nationales visées à l'article 27 et réservé au personnel dûment autorisé.

5. Les données ne peuvent être utilisées à des fins administratives. Par dérogation, les données introduites en conformité avec le présent règlement peuvent être utilisées conformément à la législation nationale de chaque État membre par les autorités visées à l'article 27, paragraphe 3, pour l'accomplissement de leurs missions.

6. t enregistrées conformément à l'article 24 du présent règlement et les données concernant des documents relatifs à des personnes qui sont enregistrées en vertu de l'article 38, paragraphe 2, points d) et e), de la ►C1 décision 2007/533/JAI ◄ peuvent être utilisées en conformité avec le droit national de chaque État membre aux fins visées à l'article 27, paragraphe 3, du présent règlement.

7. Toute utilisation de données non conforme aux paragraphes 1 à 6 sera considérée comme 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 SIS II en application du présent règlement ainsi que tout changement à cette liste. Cette 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 communautaire ne prévoie pas de dispositions particulières, le droit de chaque État membre est applicable aux données intégrées dans son N-SIS II.

Article 32

Données du SIS II et fichiers nationaux

1. L'article 31, paragraphe 2, n'affecte pas le droit qu'a un État membre de conserver dans ses fichiers nationaux 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 de trois ans au maximum, sauf si des dispositions particulières en droit national prévoient une durée de conservation plus longue.

2. L'article 31, 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 33

Information en cas d'inexécution d'un signalement

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

▼B

Article 34

Qualité des données traitées dans le SIS II

1. Un État membre signalant est responsable de l'exactitude et de l'actualité des données, ainsi que de la licéité de leur introduction dans le SIS 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'éléments indiquant qu'une donnée est entachée d'erreur de droit ou de fait, il en informe ce dernier 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 36.

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 à cette fin avec l'État membre qui a introduit le premier signalement. L'accord est réalisé sur la base d'un échange d'informations supplémentaires.

Article 35

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 l'autorité pour vérifier s'il s'agit ou non de la même personne;

▼B

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 34, 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 36

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 effets négatifs résultant d'une erreur d'identification.

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

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

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

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

a) les nom(s) et prénom(s), le(s) nom(s) à la naissance et les noms utilisés antérieurement ainsi que les 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.

▼B

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 51, paragraphe 2, 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 37

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 le présent règlement. Les autorités ne disposant pas d'un droit d'accès à certaines catégories de signalements ne doivent pas pouvoir prendre connaissance du lien vers un signalement auquel elles n'ont pas accès.

4. Un État membre met en relation des signalements 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 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 visée à l'article 51, paragraphe 2, sans préjudice des dispositions de l'instrument établissant l'instance gestionnaire.

▼B

Article 38

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'informations échangées 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 à un signalement sur la base duquel la conduite à tenir demandée a été exécutée sur son territoire. Le délai pendant lequel les données peuvent être conservées dans ces fichiers est régi par la législation nationale.

Article 39

Transfert de données à caractère personnel à des tiers

Les données traitées dans le SIS II conformément au présent règlement ne sont pas transférées à des pays tiers ou à des organisations internationales ni mises à leur disposition.

CHAPITRE VI

PROTECTION DES DONNÉES

Article 40

Traitement des catégories de données sensibles

Le traitement des catégories de données visées à l'article 8, paragraphe 1, de la directive 95/46/CE est interdit.

Article 41

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 en vertu du présent règlement s'exerce dans le respect du droit de l'État membre auprès duquel elle le fait valoir.

▼B

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 cette non-communication est indispensable à l'exécution d'une tâche légale en liaison avec le signalement ou à la protection des droits et libertés des tiers.

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 42

Droit à l'information

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

2. Cette information n'est pas fournie:

a) lorsque

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

et

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

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

▼B

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

Article 43

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 48.

▼C1

3. Les modalités de recours prévues dans le présent article sont évaluées par la Commission pour le 17 janvier 2009 au plus tard.

▼B

Article 44

Contrôle du N. SIS II

1 La ou les autorités désignées dans chaque État membre et investies des pouvoirs visés à l'article 28 de la directive 95/46/CE (les «autorités de contrôle nationales») contrôlent en toute indépendance la licéité du traitement des données à caractère personnel dans le cadre du SIS II sur leur territoire et leur transmission à partir de celui-ci, y compris pour ce qui concerne l'échange et le traitement ultérieur d'informations supplémentaires.

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

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

Article 45

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

▼B

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 46

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 ses 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 du présent règlement, 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 aux fins visées au paragraphe 2, 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 47

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) n° 45/2001.

▼B

CHAPITRE VII

RESPONSABILITÉ ET SANCTIONS

Article 48

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 au présent règlement.

3. Si le non-respect, par un État membre, des obligations qui lui incombent en vertu du présent règlement 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 49

Sanctions

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

CHAPITRE VIII

DISPOSITIONS FINALES

Article 50

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,

▼B

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 du présent règlement en ce qui concerne le SIS II central et sur la sécurité offerte par 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.

8. Au cours d'une période transitoire avant que l'instance gestionnaire n'assume ses responsabilités, la Commission est chargée d'élaborer et de présenter les rapports visés aux paragraphes 3 et 4.

Article 51

Comité

1. La Commission est assistée par un comité.

2. Dans le cas où il est fait référence au présent paragraphe, les articles 5 et 7 de la décision 1999/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.

Le délai prévu à l'article 5, paragraphe 6, de la décision 1999/468/CE est fixé à trois mois.

3. Le comité exerce ses fonctions à partir de la date d'entrée en vigueur du présent règlement.

Article 52

Modification des dispositions de l'acquis de Schengen

1. Dans les domaines relevant du traité, le présent règlement remplace, à la date visée à l'article 55, paragraphe 2, les dispositions des articles 92 à 119 de la convention de Schengen, à l'exception de son article 102 bis.

▼B

2. Il remplace aussi, à la date visée à l'article 55, 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 28 avril 1999 concernant les dépenses d'installation du C. SIS (SCH/Com-ex (99) 4);

f) décision du Comité exécutif du 28 avril 1999 concernant la mise à jour du Manuel SIRENE (SCH/Com-ex (99) 5);

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

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

i) 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, 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 au présent règlement.

Article 53

Abrogation

Le règlement (CE) n° 378/2004, le règlement (CE) n° 871/2004, la décision 2005/451/JAI, la décision 2005/728/JAI et la décision 2006/628/CE sont abrogés à la date visée à l'article 55, paragraphe 2.

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

▼B

Article 54

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 à compter de la date visée à l'article 55, paragraphe 2, les dispositions du présent règlement. Au cours de cette période transitoire, les États membres peuvent continuer à appliquer les dispositions des articles 94 et 96 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 du présent règlement 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 du présent règlement, sans retarder les actions à mener sur la base dudit signalement.

2. À la date fixée conformément à l'article 55, paragraphe 2, le reliquat du budget approuvé conformément à l'article 119 de la convention de Schengen est remboursé aux États membres. Les montants à restituer sont calculés sur la base des quotes-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 le présent règlement, par instance gestionnaire, on entend la Commission.

Article 55

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

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

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

▼B

3. Les dates visées au paragraphe 2 sont arrêtées après que:

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.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les État membres, conformément au traité instituant la Communauté européenne.