DÉCISION DE LA COMMISSION

du 4 mai 2010

établissant un plan de sécurité pour le SIS II central et l'infrastructure de communication

(2010/261/UE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le 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) [1], et notamment son article 16,

vu la 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) [2], et notamment son article 16,

considérant ce qui suit:

(1) L'article 16 du règlement (CE) nº 1987/2006 et l'article 16 de la décision 2007/533/JAI prévoient que l'instance gestionnaire et la Commission adoptent, respectivement pour le SIS II central et l'infrastructure de communication, les mesures nécessaires, y compris un plan de sécurité.

(2) L'article 15, paragraphe 4, du règlement (CE) nº 1987/2006 et l'article 15, paragraphe 4, de la décision 2007/533/JAI disposent qu'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.

(3) L'instance gestionnaire n'ayant pas encore été établie, le plan de sécurité que doit adopter la Commission devrait s'appliquer également au SIS II central pendant une période transitoire.

(4) Le règlement (CE) nº 45/2001 du Parlement européen et du Conseil [3] s'applique au traitement de données à caractère personnel par la Commission dans l'exercice de ses fonctions dans le cadre de la gestion opérationnelle du SIS II.

(5) L'article 15, paragraphe 7, du règlement (CE) nº 1987/2006 et l'article 15, paragraphe 7, de la décision 2007/533/JAI prévoient que dans le cas où la Commission délègue sa responsabilité au cours de la période transitoire avant que l'instance gestionnaire n'assume ses responsabilités, elle veille à ce que cette délégation ne porte pas préjudice à tout mécanisme permettant un contrôle effectif exercé, en vertu du droit de l'Union, par la Cour de justice, la Cour des comptes ou le Contrôleur européen de la protection des données.

(6) L'instance gestionnaire devra adopter son propre plan de sécurité pour le SIS II central lorsqu'elle prendra ses fonctions. Le plan de sécurité visé par la présente décision devra donc expirer, dans la mesure où il concerne le SIS II central, lorsque l'instance gestionnaire prendra ses fonctions.

(7) L'article 4, paragraphe 3, du règlement (CE) nº 1987/2006 et l'article 4, paragraphe 3, de la décision 2007/533/JAI prévoient que 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).

(8) Il convient que le plan de sécurité prévoie un responsable de la sécurité du système, qui assumera les tâches liées à la sécurité tant du SIS II central que de l'infrastructure de communication, ainsi que deux responsables locaux de la sécurité, qui assumeront les tâches liées à la sécurité du SIS II central et de l'infrastructure de communication, respectivement. Les rôles des responsables de la sécurité doivent être définis de manière à s'assurer que les incidents de sécurité fassent l'objet d'une réaction et d'un signalement rapides.

(9) Il y a lieu d'établir une politique de sécurité décrivant précisément tous les aspects techniques et organisationnels, conformément aux dispositions de la présente décision.

(10) Des mesures doivent être définies pour garantir le fonctionnement du SIS II central et de l'infrastructure de communication à un niveau de sécurité adéquat,

[1] JO L 381 du 28.12.2006, p. 4.
[2] JO L 205 du 7.8.2007, p. 63.
[3] JO L 8 du 12.1.2001, p. 1.

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

1. La présente décision établit l'organisation de la sécurité et les mesures de sécurité (plan de sécurité) pour la protection du SIS II central et des données qui y sont traitées contre les menaces pesant sur leur disponibilité, leur intégrité et leur confidentialité, au sens de l'article 16, paragraphe 1, du règlement (CE) nº 1987/2006, et de l'article 16, paragraphe 1, de la décision 2007/533/JAI sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) au cours d'une période transitoire avant que l'instance gestionnaire n'assume ses responsabilités.

2. La présente décision établit l'organisation de la sécurité et les mesures de sécurité (plan de sécurité) pour la protection de l'infrastructure de communication contre les menaces pesant sur sa disponibilité, son intégrité et sa confidentialité, au sens de l'article 16 du règlement (CE) nº 1987/2006, et de l'article 16 de la décision 2007/533/JAI sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

CHAPITRE II

ORGANISATION, RESPONSABILITÉS ET GESTION DES INCIDENTS

Article 2

Tâches de la Commission

1. La Commission met en œuvre les mesures de sécurité applicables au SIS II central visées dans la présente décision et en contrôle l'efficacité.

2. La Commission met en œuvre les mesures de sécurité applicables à l'infrastructure de communication visées dans la présente décision et en contrôle l'efficacité.

3. La Commission désigne parmi ses agents un responsable de la sécurité du système. Le responsable de la sécurité du système est nommé par le directeur général de la direction générale de la justice, de la liberté et de la sécurité de la Commission. Ses tâches consistent en particulier:

a) à élaborer la politique de sécurité telle que décrite à l'article 7 de la présente décision;

b) à contrôler l'efficacité de la mise en œuvre des procédures de sécurité applicables au SIS II central;

c) à contrôler l'efficacité de la mise en œuvre des procédures de sécurité applicables à l'infrastructure de communication;

d) à contribuer à l'élaboration de rapports sur la sécurité tels que visés à l'article 50 du règlement (CE) nº 1987/2006 et à l'article 66 de la décision 2007/533/JAI;

e) à accomplir des tâches de coordination et d'assistance dans le cadre des contrôles et audits réalisés par le Contrôleur européen de la protection des données visés à l'article 45 du règlement (CE) nº 1987/2006 et à l'article 61 de la décision 2007/533/JAI, et dans le cadre de la notification des incidents, au sens de l'article 5, paragraphe 2, au délégué à la protection des données de la Commission;

f) à veiller à ce que la présente décision et la politique de sécurité soient appliquées correctement et intégralement par tous les prestataires, y compris les sous-traitants, qui sont associés d'une manière ou d'une autre à la gestion du SIS II central;

g) à veiller à ce que la présente décision et la politique de sécurité soient appliquées correctement et intégralement par tous les contractants, y compris les sous-traitants, qui sont associés d'une manière ou d'une autre à la gestion de l'infrastructure de communication;

h) à tenir à jour une liste des points de contact nationaux uniques pour la sécurité du SIS II et à transmettre celle-ci au responsable local de la sécurité pour l'infrastructure de communication;

i) à transmettre la liste visée au point h) au responsable local de la sécurité pour le SIS II central.

Article 3

Responsable local de la sécurité pour le SIS II central

1. Sans préjudice de l'article 8, la Commission désigne parmi ses agents un responsable local de la sécurité pour le SIS II central. Il y a lieu d'éviter les conflits d'intérêt entre la fonction de responsable local de la sécurité et toute autre fonction officielle. Le responsable local de la sécurité pour le SIS II central est nommé par le directeur général de la direction générale de la justice, de la liberté et de la sécurité de la Commission.

2. Le responsable local de la sécurité pour le SIS II central veille à ce que les mesures de sécurité visées dans la présente décision soient mises en œuvre et à ce que les procédures de sécurité soient suivies dans le CS-SIS principal. En ce qui concerne le CS-SIS de secours, le responsable local de la sécurité pour le SIS II central veille en outre à ce que les mesures de sécurité visées dans la présente décision, à l'exception de celles qui sont mentionnées à l'article 9, soient mises en œuvre et à ce que les procédures de sécurité connexes soient suivies.

3. Le responsable local de la sécurité pour le SIS II central peut confier à un adjoint toute tâche parmi celles qui lui sont assignées. Il y a lieu d'éviter les conflits d'intérêt entre la fonction consistant en l'exécution de ces tâches et toute autre fonction officielle. Un numéro de téléphone unique et une adresse unique permettent de joindre à tout moment le responsable local de la sécurité ou son adjoint de service.

4. Le responsable local de la sécurité pour le SIS II central exécute les tâches découlant des mesures de sécurité à prendre sur les sites du CS-SIS principal et du CS-SIS de secours, dans les limites visées au paragraphe 1, et notamment celles qui consistent:

a) à accomplir des tâches relatives à la sécurité opérationnelle locale, y compris des audits de pare-feux, des tests de sécurité réguliers, des audits et des rapports;

b) à contrôler l'efficacité du plan de continuité des activités et à veiller à ce que des exercices réguliers soient effectués;

c) à rassembler des éléments d'information concernant tout incident survenant dans le SIS II central susceptible d'avoir un impact sur la sécurité du SIS II central ou de l'infrastructure de communication et à en faire rapport au responsable de la sécurité du système;

d) à informer le responsable de la sécurité du système lorsque la politique de sécurité doit être modifiée;

e) à veiller à ce que la présente décision et la politique de sécurité soient appliquées par tous les prestataires, y compris les sous-traitants, qui sont associés d'une manière ou d'une autre à la gestion opérationnelle du SIS II central;

f) à veiller à ce que le personnel soit informé de ses obligations et à contrôler l'application de la politique de sécurité;

g) à suivre les évolutions en matière de sécurité des technologies de l'information et à faire en sorte que le personnel reçoive une formation adaptée;

h) à rassembler des informations de base et à élaborer des scénarios pour la mise en place, l'actualisation et le réexamen de la politique de sécurité conformément à l'article 7.

Article 4

Responsable local de la sécurité pour l'infrastructure de communication

1. Sans préjudice de l'article 8, la Commission désigne parmi ses agents un responsable local de la sécurité pour l'infrastructure de communication. Il y a lieu d'éviter les conflits d'intérêt entre la fonction de responsable local de la sécurité et toute autre fonction officielle. Le responsable local de la sécurité pour l'infrastructure de communication est nommé par le directeur général de la direction générale de la justice, de la liberté et de la sécurité de la Commission.

2. Le responsable local de la sécurité pour l'infrastructure de communication contrôle le fonctionnement de celle-ci et veille à ce que les mesures de sécurité soient mises en œuvre et à ce que les procédures de sécurité soient suivies.

3. Le responsable local de la sécurité pour l'infrastructure de communication peut confier à un adjoint toute tâche parmi celles qui lui sont assignées. Il y a lieu d'éviter les conflits d'intérêt entre la fonction consistant en l'exécution de ces tâches et toute autre fonction officielle. Un numéro de téléphone unique et une adresse unique permettent de joindre à tout moment le responsable local de la sécurité ou son adjoint de service.

4. Le responsable local de la sécurité pour l'infrastructure de communication exécute les tâches découlant des mesures de sécurité la concernant, et notamment celles qui consistent:

a) à accomplir toutes les tâches relatives à la sécurité de l'infrastructure de communication, y compris des audits de pare-feux, des tests de sécurité réguliers, des audits et des rapports;

b) à contrôler l'efficacité du plan de continuité des activités et à veiller à ce que des exercices réguliers soient effectués;

c) à rassembler des éléments d'information concernant tout incident survenu dans l'infrastructure de communication susceptible d'avoir un impact sur la sécurité du SIS II central ou de l'infrastructure de communication et à en faire rapport au responsable de la sécurité du système;

d) à informer le responsable de la sécurité du système lorsque la politique de sécurité doit être modifiée;

e) à veiller à ce que la présente décision et la politique de sécurité soient appliquées par tous les prestataires, y compris les sous-traitants, qui sont associés d'une manière ou d'une autre à la gestion de l'infrastructure de communication;

f) à veiller à ce que le personnel soit informé de ses obligations et à contrôler l'application de la politique de sécurité;

g) à suivre les évolutions en matière de sécurité des technologies de l'information et à faire en sorte que le personnel reçoive une formation adaptée;

h) à rassembler des informations de base et à élaborer des scénarios pour la mise en place, l'actualisation et le réexamen de la politique de sécurité conformément à l'article 7.

Article 5

Incidents de sécurité

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

2. Les incidents de sécurité sont gérés de telle sorte qu'une réponse rapide, efficace et idoine y soit apportée, dans le respect de la politique de sécurité. Des procédures sont définies pour remédier à tout incident.

3. Les informations relatives à un incident de sécurité ayant ou pouvant avoir un impact sur le fonctionnement du SIS II dans un État membre ou sur la disponibilité, l'intégrité et la confidentialité des données saisies ou envoyées par un État membre sont communiquées à l'État membre concerné. Les incidents de sécurité sont notifiés au Contrôleur de la protection des données de la Commission.

Article 6

Gestion des incidents

1. L'ensemble du personnel et des prestataires associés au développement, à la gestion ou au fonctionnement du SIS II sont tenus de consigner toute faille de sécurité observée ou suspectée dans l'infrastructure de communication et de signaler celle-ci au responsable de la sécurité du système ou au responsable local de la sécurité pour l'infrastructure de communication.

2. Lorsqu'un incident ayant ou pouvant avoir un impact sur la sécurité du fonctionnement du SIS II est détecté, le responsable local de la sécurité pour l'infrastructure de communication informe dès que possible le responsable de la sécurité du système et, le cas échéant, le point de contact national unique pour la sécurité du SIS II, s'il existe dans l'État membre en question, par écrit ou, en cas d'extrême urgence, par une autre voie de communication. Le rapport comporte une description de l'incident de sécurité, indique le niveau de risque et les répercussions éventuelles et cite les mesures qui ont été ou devraient être prises pour atténuer le risque.

3. Le responsable local de la sécurité pour l'infrastructure de communication se procure immédiatement tous les éléments d'information relatifs à l'incident de sécurité. Dans la mesure autorisée par les dispositions applicables en matière de protection des données, ces éléments d'information sont communiqués au responsable de la sécurité du système s'il en fait la demande.

4. La politique de sécurité définit des procédures de retour d'information garantissant que le responsable de la sécurité du système et le responsable local de la sécurité pour l'infrastructure de communication soient informés de la nature, du traitement et de l'issue de l'incident de sécurité dès que celui-ci est réglé et clos.

5. Les paragraphes 1 à 4 s'appliquent mutatis mutandis aux incidents concernant le SIS II central. Dans ce contexte, toute référence au responsable local de la sécurité pour l'infrastructure de communication aux paragraphes 1 à 4 doit s'entendre comme une référence au responsable local de la sécurité pour le SIS II central.

CHAPITRE III

MESURES DE SÉCURITÉ

Article 7

Politique de sécurité

1. Le directeur général de la direction générale de la justice, de la liberté et de la sécurité définit, actualise et réexamine régulièrement une politique de sécurité contraignante conformément à la présente décision. La politique de sécurité prévoit dans le détail les procédures et les mesures de protection contre les menaces pesant sur la disponibilité, l'intégrité et la confidentialité de l'infrastructure de communication, y compris un plan d'urgence pour garantir le niveau de sécurité adéquat qui est prescrit dans la présente décision. Cette politique se conforme à la présente décision.

2. La politique de sécurité s'appuie sur une appréciation des risques. Les mesures décrites dans la politique de sécurité sont proportionnées aux risques recensés.

3. L'appréciation des risques et la politique de sécurité sont actualisées si des évolutions technologiques, la découverte de nouvelles menaces ou d'autres circonstances l'exigent. La politique de sécurité est réexaminée en tout état de cause chaque année, pour s'assurer qu'elle constitue encore une réponse adéquate compte tenu de la dernière appréciation des risques en date ou de toute évolution technologique, menace ou autre circonstance pertinente récemment révélée.

4. La politique de sécurité est élaborée par le responsable de la sécurité du système, en collaboration avec le responsable local de la sécurité pour le SIS II central et le responsable local de la sécurité pour l'infrastructure de communication.

5. Les paragraphes 1 à 4 s'appliquent mutatis mutandis à la politique de sécurité pour le SIS II central. Dans ce contexte, toute référence au responsable local de la sécurité pour l'infrastructure de communication aux paragraphes 1 à 4 doit s'entendre comme une référence au responsable local de la sécurité pour le SIS II central.

Article 8

Mise en œuvre des mesures de sécurité

1. L'exécution des tâches et la mise en œuvre des exigences définies dans la présente décision et dans la politique de sécurité, y compris la tâche de désigner un responsable local de la sécurité, peuvent être sous-traitées ou confiées à des organismes privés ou publics.

2. Dans ce cas, la Commission veille, par la conclusion d'un accord juridiquement contraignant, à ce que les exigences énoncées dans la présente décision et dans la politique de sécurité soient pleinement respectées. Si la désignation d'un responsable local de la sécurité est déléguée ou sous-traitée, la Commission s'assure, par la conclusion d'un accord juridiquement contraignant, d'être consultée au sujet de la personne qui sera désignée à cette fonction.

Article 9

Contrôle de l'accès aux installations

1. Des périmètres de sécurité délimités d'une manière appropriée par des barrières et des postes de contrôle des entrées sont mis en place pour protéger les zones qui accueillent des installations de traitement des données.

2. Des zones sécurisées sont établies à l'intérieur des périmètres de sécurité pour protéger les éléments physiques (biens matériels), y compris le matériel informatique, les supports de données et les consoles, les plans et autres documents relatifs au SIS II, ainsi que les bureaux et autres lieux de travail du personnel assurant le fonctionnement du SIS II. Ces zones sécurisées sont protégées par des postes appropriés de contrôle des entrées, de manière à ce que seul le personnel autorisé puisse y accéder. Dans les zones sécurisées, le travail est soumis à des règles de sécurité minutieuses exposées dans la politique de sécurité.

3. Des dispositifs sont prévus et mis en place pour assurer la sécurité matérielle des bureaux, locaux et installations. Les points d'accès tels que les zones de livraison et de chargement et d'autres points par lesquels des personnes non autorisées sont susceptibles de pénétrer dans les locaux sont contrôlés et, si possible, isolés des installations de traitement des données afin d'empêcher tout accès non autorisé.

4. Des mesures sont élaborées pour assurer la protection physique des périmètres de sécurité contre les dommages susceptibles de résulter d'une catastrophe naturelle ou d'origine humaine et sont appliquées proportionnellement au risque.

5. Les équipements sont protégés contre les menaces physiques et environnementales et contre toute possibilité d'accès non autorisé.

6. Si elle dispose d'informations à cet égard, la Commission ajoute à la liste visée à l'article 2, paragraphe 3, point h), un point de contact unique pour le contrôle de l'application des dispositions du présent article dans les locaux abritant le CS-SIS de secours.

Article 10

Supports de données et contrôle des biens matériels

1. Les supports amovibles contenant des données sont protégés contre l'accès non autorisé, l'utilisation frauduleuse ou la corruption et leur lisibilité est assurée tout au long du cycle de vie des données.

2. Les supports sont jetés par des voies sécurisées lorsqu'ils ne sont plus utiles, conformément aux procédures détaillées exposées dans la politique de sécurité.

3. Des inventaires garantissent la disponibilité d'informations relatives au lieu de stockage, à la durée de conservation applicable et aux autorisations d'accès.

4. Tous les biens matériels importants de l'infrastructure de communication sont inventoriés de manière à ce qu'ils puissent être protégés selon leur importance. Un registre actualisé des équipements informatiques pertinents est tenu.

5. Une documentation actualisée relative à l'infrastructure de communication est fournie. Celle-ci doit être protégée contre l'accès non autorisé.

6. Les paragraphes 1 à 5 s'appliquent mutatis mutandis au SIS II central. Dans ce contexte, toute référence à l'infrastructure de communication s'entend comme une référence au SIS II central.

Article 11

Contrôle du stockage

1. Des mesures adéquates sont prises pour assurer un stockage idoine des données et prévenir tout accès non autorisé à celles-ci.

2. Tous les équipements contenant des supports de stockage font l'objet d'une vérification avant que ces derniers ne soient jetés, pour s'assurer que les données sensibles en ont été retirées ou ont été totalement écrasées, ou ils sont détruits par des voies sécurisées.

Article 12

Contrôle des mots de passe

1. Tous les mots de passe sont conservés en lieu sûr et font l'objet d'un traitement confidentiel. En cas de suspicion de divulgation d'un mot de passe, il y a lieu de modifier celui-ci immédiatement ou de désactiver le compte concerné. Les identifiants attribués aux utilisateurs sont uniques et individuels.

2. La politique de sécurité définit des procédures de connexion et de déconnexion, afin d'empêcher tout accès non autorisé.

Article 13

Contrôle des accès

1. La politique de sécurité prévoit une procédure formelle pour l'enregistrement du personnel en poste et l'annulation de cet enregistrement, lui accordant ou lui retirant le droit d'accéder au matériel informatique et aux logiciels du SIS II aux fins de la gestion opérationnelle. L'attribution et l'utilisation d'identifiants d'accès adéquats (mots de passe ou autres moyens appropriés) sont contrôlées par une procédure de gestion formelle définie dans la politique de sécurité.

2. L'accès au matériel informatique et aux logiciels du SIS II sur le site du CS-SIS:

i) est limité aux personnes autorisées;

ii) est limité aux cas dans lesquels un besoin légitime d'accéder au système peut être déterminé, conformément à l'article 45 du règlement (CE) nº 1987/2006 et à l'article 61 de la décision 2007/533/JAI, ou à l'article 50, paragraphe 2, dudit règlement et à l'article 66, paragraphe 2, de ladite décision;

iii) n'excède pas la durée et la portée nécessaires à son objet; et

iv) se déroule dans le respect d'une politique de contrôle des accès qui doit être définie dans la politique de sécurité.

3. Seuls les logiciels et les consoles autorisés par le responsable local de la sécurité pour le SIS II central sont utilisés sur le site du CS-SIS. Le recours à des utilitaires système capables de passer outre aux contrôles des systèmes et des applications est restreint et contrôlé. Des procédures sont mises en place pour contrôler l'installation des logiciels.

Article 14

Contrôle des communications

L'infrastructure de communication fait l'objet d'un suivi pour garantir la disponibilité, l'intégrité et la confidentialité des échanges d'information. Des procédés cryptographiques sont utilisés pour protéger les données transmises dans l'infrastructure de communication.

Article 15

Contrôle des enregistrements de données

Les comptes des personnes autorisées à accéder aux logiciels du SIS II à partir du CS-SIS sont contrôlés par le responsable local de la sécurité pour le SIS II central. L'utilisation de ces comptes est enregistrée, y compris la date et l'heure ainsi que l'identité de l'utilisateur.

Article 16

Contrôle des transports

1. Des mesures adéquates sont élaborées dans la politique de sécurité pour empêcher l'accès non autorisé aux données à caractère personnel, leur copie, leur modification ou leur effacement au cours de leur transmission vers le SIS II ou en provenance de celui-ci ou pendant le transport des supports de données. Des dispositions de la politique de sécurité définissent les types admissibles d'envoi ou de transport et les procédures permettant d'établir les responsabilités relatives au transport d'éléments et à leur arrivée au lieu de destination. Les supports de données ne contiennent pas de données autres que celles qui doivent être envoyées.

2. Les services fournis par des tiers qui impliquent d'accéder à des données, de les traiter, de les communiquer, ou de gérer des installations de traitement des données, ou de contribuer à l'ajout de produits ou de services dans de telles installations, font l'objet de contrôles de sécurité intégrés et appropriés.

Article 17

Sécurité de l'infrastructure de communication

1. L'infrastructure de communication est gérée et contrôlée d'une manière adéquate afin de la protéger contre d'éventuelles menaces et pour assurer sa sécurité ainsi que celle du SIS II central, y compris des données échangées par son intermédiaire.

2. Des dispositifs de sécurité, des niveaux de service et des exigences en matière de gestion sont définis pour tous les services de réseau dans l'accord relatif aux services de réseau conclu avec le prestataire de services.

3. Outre la protection des points d'accès au SIS II, tout autre service utilisé par l'infrastructure de communication est également protégé. Des mesures adéquates sont définies dans la politique de sécurité.

Article 18

Contrôle

1. Les journaux contenant les informations visées à l'article 18, paragraphe 1, du règlement (CE) nº 1987/2006 et à l'article 18, paragraphe 1, de la décision 2007/533/JAI relatives à chaque accès au CS-SIS et à tous les échanges de données à caractère personnel dans celui-ci sont conservés en toute sécurité et accessibles dans les locaux abritant le CS-SIS central principal et le CS-SIS de secours pendant la période maximale visée à l'article 18, paragraphe 3, dudit règlement et à l'article 18, paragraphe 3, de ladite décision.

2. Les procédures de contrôle de l'utilisation des installations de traitement des données ou des défaillances de celles-ci sont exposées dans la politique de sécurité et les résultats des activités de contrôle sont examinés régulièrement. En cas de besoin, des mesures appropriées sont prises.

3. Les dispositifs de journalisation et les journaux sont protégés contre la falsification ou l'accès non autorisé, afin de satisfaire aux exigences en matière de collecte et de consignation pendant la période de conservation des données.

Article 19

Procédés cryptographiques

Des procédés cryptographiques sont utilisés au besoin pour assurer la protection des informations. Le recours à ces procédés, ainsi que les buts et les conditions dans lesquels ils sont appliqués doivent être approuvés au préalable par le responsable de la sécurité du système.

CHAPITRE IV

SÉCURITÉ DES RESSOURCES HUMAINES

Article 20

Profils des membres du personnel

1. La politique de sécurité définit les fonctions et responsabilités des personnes autorisées à accéder au SIS II central.

2. La politique de sécurité définit les fonctions et responsabilités des personnes autorisées à accéder à l'infrastructure de communication.

3. Les rôles et responsabilités en matière de sécurité incombant aux agents de la Commission, aux prestataires et au personnel associés à la gestion opérationnelle sont définis, décrits et communiqués aux personnes concernées. La description des postes et des objectifs précise les rôles et responsabilités dévolus aux agents de la Commission; des contrats ou accords de niveau de service définissent ceux qui sont attribués aux prestataires.

4. Des accords de confidentialité sont conclus avec toutes les personnes qui ne sont pas soumises aux règles du service public d'un État membre ou du service public de l'Union européenne. Le personnel chargé de traiter des données provenant du SIS II dispose de l'autorisation ou de la certification nécessaire, conformément aux procédures détaillées exposées dans la politique de sécurité.

Article 21

Information du personnel

1. Tous les membres du personnel et tous les prestataires reçoivent une formation adéquate dans le domaine la sensibilisation à la sécurité, des prescriptions juridiques, des politiques et des procédures, dans la mesure nécessaire pour l'exercice de leurs fonctions.

2. S'agissant d'un emploi ou d'un contrat qui prend fin, la politique de sécurité définit les responsabilités liées au changement de poste ou à la cessation de la fonction incombant aux membres du personnel et aux prestataires; la politique de sécurité définit également des procédures pour la restitution des biens matériels et le retrait des droits d'accès.

CHAPITRE V

DISPOSITION FINALE

Article 22

Applicabilité

1. La présente décision est applicable à partir de la date fixée par le Conseil conformément à l'article 55, paragraphe 2, du règlement (CE) n° 1987/2006 et à l'article 71, paragraphe 2, de la décision 2007/533/JAI.

2. L'article 1er, paragraphe 1, l'article 2, paragraphe 1, l'article 2, paragraphe 3, points b), d), f) et i), l'article 3, l'article 6, paragraphe 5, l'article 7, paragraphe 5, l'article 9, paragraphe 6, l'article 10, paragraphe 6, l'article 13, paragraphes 2 et 3, l'article 15, l'article 18 et l'article 20, paragraphe 1, expirent lorsque l'instance gestionnaire prend ses fonctions.

Fait à Bruxelles, le 4 mai 2010.

Par la Commission

Le président

José Manuel BARROSO