DÉCISION DE LA COMMISSION

du 4 mai 2010

établissant un plan de sécurité pour le fonctionnement du système d'information sur les visas

(2010/260/UE)

LA COMMISSION EUROPÉENNE,

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

vu le règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) [1], et notamment son article 32,

considérant ce qui suit:

(1) L'article 32, paragraphe 3, du règlement (CE) nº 767/2008 prévoit que l'instance gestionnaire prend les mesures nécessaires à la réalisation des objectifs fixés en matière de sécurité à l'article 32, paragraphe 2, en ce qui concerne le fonctionnement du VIS, y compris l'établissement d'un plan de sécurité.

(2) L'article 26, paragraphe 4, du règlement (CE) nº 767/2008 dispose qu'au cours d'une période transitoire avant que l'instance gestionnaire n'entre en fonction, la Commission est chargée de la gestion opérationnelle du VIS.

(3) Le règlement (CE) nº 45/2001 du Parlement européen et du Conseil [2]s'applique au traitement des données à caractère personnel par la Commission dans l'exercice de ses fonctions dans le cadre de la gestion opérationnelle du VIS.

(4) L'article 26, paragraphe 7, du règlement (CE) nº 767/2008 prévoit que dans le cas où la Commission délègue sa responsabilité au cours de la période transitoire avant que l'instance gestionnaire n'entre en fonction, 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 de l'Union, par la Cour de justice, la Cour des comptes ou le Contrôleur européen de la protection des données.

(5) L'instance gestionnaire devra établir son propre plan de sécurité applicable au VIS dès qu'elle aura pris ses fonctions.

(6) La décision 2008/602/CE de la Commission du 17 juin 2008 définissant l'architecture physique ainsi que les caractéristiques des interfaces nationales et de l'infrastructure de communication entre le système central d'information sur les visas et les interfaces nationales pour la phase de développement [3] décrit les services de sécurité requis pour le réseau du VIS.

(7) L'article 27 du règlement (CE) nº 767/2008 dispose que le VIS central principal, qui assure des fonctions de contrôle et de gestion techniques, est installé à Strasbourg (France), et un VIS central de secours, capable d'assurer l'ensemble des fonctionnalités du VIS central principal en cas de défaillance du système, est installé à Sankt Johann im Pongau (Autriche).

(8) 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 efficaces et rapides.

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

(10) Des mesures doivent être définies pour garantir le fonctionnement du VIS à un niveau de sécurité adéquat,

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

La présente décision définit l'organisation de la sécurité et les mesures de sécurité (plan de sécurité) au sens de l'article 32, paragraphe 3, du règlement (CE) nº 767/2008.

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 VIS central et à l'infrastructure de communication visées dans la présente décision et en contrôle l'efficacité.

[1] JO L 218 du 13.8.2008, p. 60.
[2] JO L 8 du 12.1.2001, p. 1.
[3] JO L 194 du 23.7.2008, p. 3.

2. 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, actualiser et adapter 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 VIS central et à l'infrastructure de communication;

c) à contribuer à l'élaboration de rapports sur la sécurité tels que visés à l'article 50, paragraphes 3 et 4, du règlement (CE) nº 767/2008;

d) 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 42 du règlement (CE) nº 767/2008;

e) 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 et au fonctionnement du VIS;

f) à tenir à jour une liste de points de contact nationaux uniques pour la sécurité du VIS et à transmettre celle-ci aux responsables locaux de la sécurité du VIS central et de l'infrastructure de communication.

Article 3

Responsable local de la sécurité pour le VIS central

1. Sans préjudice de l'article 8, la Commission désigne parmi ses agents un responsable local de la sécurité pour le VIS 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 VIS 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 VIS 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 VIS central principal. En ce qui concerne le VIS central de secours, le responsable local de la sécurité pour le VIS central veille à ce que les mesures de sécurité visées dans la présente décision, à l'exception de celles qui sont mentionnées à l'article 10, soient mises en œuvre et à ce que les procédures de sécurité connexes soient suivies.

3. Le responsable local de la sécurité pour le VIS 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 VIS central exécute les tâches découlant des mesures de sécurité à prendre sur le site principal et le site de secours du VIS central, 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 susceptible d'avoir un impact sur la sécurité du VIS 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 et au fonctionnement du VIS 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 relatives à celle-ci, et notamment celles qui consistent:

a) à accomplir toutes les tâches relatives à la sécurité de l'infrastructure de communication, telles que 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 susceptible d'avoir un impact sur la sécurité de l'infrastructure de communication ou du VIS central ou sur les systèmes nationaux, 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 fonctionnement du VIS 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. La politique de sécurité définit des procédures pour remédier à tout incident. 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.

3. Les informations relatives à un incident de sécurité ayant ou pouvant avoir un impact sur le fonctionnement du VIS dans un État membre ou sur la disponibilité, l'intégrité et la confidentialité des données saisies dans le VIS 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 VIS sont tenus de consigner toute faille de sécurité observée ou suspectée dans le fonctionnement du VIS et de signaler celle-ci au responsable de la sécurité du système, au responsable local de la sécurité pour le VIS central ou au responsable local de la sécurité pour l'infrastructure de communication, selon le cas.

2. Lorsqu'un incident ayant ou pouvant avoir un impact sur la sécurité du fonctionnement du VIS est détecté, le responsable local de la sécurité pour le VIS central ou 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 VIS, 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 le VIS central ou le responsable local de la sécurité pour l'infrastructure de communication, selon le cas, 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. Des procédures de retour d'information sont mises en place pour garantir la transmission des résultats dès que l'incident est réglé et clos.

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 du VIS, 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 VIS et le responsable local de la sécurité pour l'infrastructure de communication.

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 VIS, ainsi que les bureaux et autre lieux de travail du personnel assurant le fonctionnement du VIS. 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 aux règles de sécurité détaillées prévues 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 2, point f), un point de contact unique pour le contrôle de l'application des dispositions du présent article dans les locaux abritant le VIS central 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 du VIS central et 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 au VIS central et à l'infrastructure de communication est fournie. Celle-ci doit être protégée contre l'accès non autorisé.

Article 11

Contrôle du stockage

1. Des mesures adéquates sont prises pour assurer un stockage idoine des informations 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 de l'utilisateur. 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 VIS sur le site du VIS central 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 VIS sur le site du VIS central

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 42 et à l'article 50, paragraphe 2, du règlement (CE) nº 767/2008;

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 VIS central sont utilisés sur le site du VIS central. 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 VIS à partir du VIS central sont contrôlés par le responsable local de la sécurité pour le VIS 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 VIS 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 VIS 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 VIS, tout autre service utilisé par l'infrastructure de communication est également protégé. Des mesures adéquates sont définies dans la politique de sécurité.

Article 18

Contrôles

1. Les journaux contenant les informations visées à l'article 34, paragraphe 1, du règlement (CE) nº 767/2008, relatives à chaque accès au VIS central et à toutes les opérations de traitement de données dans celui-ci, sont conservés en lieu sûr et sont accessibles dans les locaux abritant le VIS central principal et le VIS central de secours pendant la période visée à l'article 34, paragraphe 2, dudit règlement.

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 VIS, et notamment à l'infrastructure de communication.

2. 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.

3. 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 VIS 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, le cas échéant, 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 la Commission conformément à l'article 48, paragraphe 1, du règlement (CE) nº 767/2008.

2. La présente décision expire lorsque l'instance gestionnaire prend ses fonctions.

Fait à Bruxelles, le 4 mai 2010.

Par la Commission

Le président

José Manuel BARROSO