Avis sur une notification de contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant le dossier «Système de contrôle d'accès physique (PACS) de la Commission: Projet de sécurisation globale (PSG)»

Bruxelles, le 8 septembre 2011 (Dossier 2010-0427)

1. Procédure

Le 3 juin 2010, le contrôleur européen de la protection des données (**CEPD**) a reçu du délégué à la protection des données (**DPD**) de la Commission européenne une notification de contrôle préalable sur le traitement de données à caractère personnel dans le contexte du système de contrôle d'accès physique (PACS) de la Commission.

Le CEPD a également reçu divers documents en rapport avec cette notification, qui ont été publiés sur l'intranet de la Commission, à savoir:

1. Document de vision du «Projet de sécurisation globale» (PSG)
2. Document d'architecture du PSG
3. Rapport sur les recommandations et les options technologiques du PSG
4. Cas d'utilisation du contrôle d'accès physique du PSG et scénarios de traitement de données
5. Système d'information et applications du PSG
6. Destinataires du traitement
7. Délais de verrouillage/effacement des données
8. Information des visiteurs
9. Information des nouveaux détenteurs de badges

Dans le cadre du PSG, l'établissement d'un site de pré-production a été jugé nécessaire pour pouvoir valider et perfectionner les divers options, systèmes et mesures technologiques proposés aux fins de la mise en œuvre du nouveau système de contrôle d'accès physique (PACS) au sein de la Commission européenne. En accord avec sa pratique de contrôle préalable des projets pilotes, le CEPD a mis en place une procédure relative aux projets pilotes/à la pré-production en ce qui concerne les nouvelles opérations de traitement technologiques et la Commission a suivi cette procédure.

Dans cette procédure, le CEPD avait demandé à la Commission de lui fournir certaines informations sur la phase de pré-production et avait analysé les traitements concernés. Dans une lettre datée du 21 octobre 2010, antérieure au lancement de la phase de pré-production, le CEPD a formulé des recommandations spécifiques au projet pilote. Il a par ailleurs émis des recommandations dont il fallait tenir compte à l'occasion de la mise en service complète du système, afin d'éviter toute contradiction entre les deux phases (phase pilote et mise en service complète du système) susceptible d'entraîner une violation du principe de protection des données à caractère personnel.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
Courriel: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

Cette phase de pré-production a eu lieu de novembre 2010 à mai 2011 et le responsable du traitement a transmis les résultats au CEPD le 1er juillet 2011.

À cette occasion, le DPD a fourni au CEPD deux documents supplémentaires:

- un rapport d'évaluation du site de pré-production;
- un document sur les cas d'utilisation (scénarios) du contrôle d'accès physique du PSG et les scénarios de traitement des données modifiés, qui reflète les modifications adoptées au terme de la phase de pré-production.

Les conclusions de la phase de pré-production ont été synthétisées dans le rapport par le responsable du traitement, lequel signale que *«globalement, toutes les options et technologies prévues ont été validées et jugées adéquates aux fins prévues et la mise en place des fonctionnalités requises, conformément aux plans et à la conception. Pour l'essentiel, les principales adaptations qui devaient ou devront être réalisées ont été programmées au niveau de l'exploitation ou de la procédure opérationnelle»*.

Au terme de la phase de pré-production, le PACS est resté opérationnel dans le bâtiment qui était utilisé en tant que site de pré-production (L-56), dans le respect des conditions établies pour sa mise en œuvre (information, conservation, etc.).

Le présent avis de contrôle préalable clôture l'analyse juridique du PACS. Le plein déploiement du PACS au sein des services de la Commission européenne à Bruxelles est prévu début 2012.

Le CEPD note que la Commission européenne a développé une approche respectueuse de la vie privée pour la mise en œuvre des opérations de traitement concernées en impliquant le CEPD dès les toutes premières phases de la procédure de notification, en mettant en place une phase pilote et en prenant en considération tous les aspects pertinents en matière de protection des données dès le début de ses travaux.

Le projet d'avis a été transmis au DPD le 29 juillet 2011 afin qu'il puisse formuler des observations. Le CEPD a reçu une réponse le 6 septembre 2011.

2. Les faits

Le système doit permettre la mise en œuvre d'un mécanisme de contrôle d'accès physique unique et cohérent pour l'ensemble de la Commission par l'exécution de toutes les fonctions de sécurité physique requises. Il s'agit d'un PACS distribué, destiné exclusivement au contrôle d'accès physique et aux fonctions de sécurité connexes.

De manière plus spécifique, il a été conçu en vue de l'automatisation du contrôle d'accès physique et de l'application uniforme des procédures et politiques de sécurité. À cette fin sont mis en œuvre les objectifs et solutions technologiques suivants:

- un système de contrôle d'accès informatisé central pour activer et gérer toutes les fonctions de contrôle d'accès physique et les définitions des droits d'accès, permettant notamment:
    - la production uniforme et commune de badges et de définitions de droits d'accès;
    - la définition d'un contrôle d'accès centralisé, la surveillance et la détection des intrusions;

- le contrôle centralisé des biens sur la base de technologies standard et de politiques communes;
- la gestion et la configuration centralisées des terminaux de contrôle d'accès;

- un badge ou une carte d'identité commune faisant appel à des technologies efficaces et uniformisées, basées sur:
  - une carte à puce de proximité sans contact, exploitant une technologie d'identification par radiofréquences (RFID) totalement compatible avec la norme internationale ISO/IEC 14443 Type A;
  - une vérification biométrique basée sur les minuties des empreintes digitales, stockées exclusivement sur la mémoire interne de la puce;
  - un ensemble distribué d'équipements de sécurité physique (p. ex. dispositifs de contrôle des portes, systèmes de prévention et de détection des intrusions, dispositifs de contrôle, vidéosurveillance, etc.).

Les fonctions et opérations du système sont décrites dans le «document de vision du PSG» et une description détaillée des cas d'utilisation du système et des scénarios de traitement de données est fournie dans le document «Cas d'utilisation du contrôle d'accès physique et scénarios de traitement de données», qui a été mis à jour au terme de la phase menée sur le site de pré-production.

Ainsi qu'il est décrit dans la notification, les **finalités** du traitement en question sont les suivantes:

1. contrôle et protection des locaux, des informations et des biens de la Commission;
2. sécurité et protection des personnes présentes à l'intérieur des locaux de la Commission;
3. conformité avec les exigences de sécurité. Il est nécessaire de connaître avec la plus grande exactitude possible le nombre de personnes encore présentes dans les locaux pour les cas d'évacuation et les autres situations de crise;
4. respect des exigences légales. Prévention, recherche, détection et condamnation des violations de mesures administratives ou disciplinaires ou d'infractions pénales (le traitement est exclusivement basé sur la collecte de données et leur transmission ultérieure aux organes compétents de la Commission).

Le traitement de données **manuel** est totalement ou pratiquement exclu. En revanche, l'utilisation de documents d'identité ou légaux par des réceptionnistes ou des opérateurs, des exceptions envisageables en cas d'indisponibilité du système et d'intervention humaine indispensable, pourraient donner lieu à un traitement manuel de données.

La base juridique des opérations de traitement se trouve, d'après la notification, dans les actes juridiques suivants:

1. la communication de la Commission sur le nouveau système d'accès et de sécurisation des immeubles de la Commission, C(2007)797 du 14 mars 2007;
2. la décision de la Commission sur les tâches et responsabilités du Bureau de sécurité, C(94) 2129 du 8 septembre 1994;
3. la responsabilité de la Commission sur la protection de son personnel (sécurité et sûreté) et de ses biens: décision 2007/65/CE de la Commission du 15 décembre 2006 sur les niveaux d'alerte et la gestion des situations de crise;
4. les dispositions de la Commission en matière de sécurité: décision 2001/844/CE/CECA/Euratom de la Commission du 29 novembre 2001 modifiant son règlement intérieur.

À la lumière des finalités décrites ci-dessus, les **personnes concernées** sont toute personne[1] ayant accès ou sollicitant l'accès aux locaux de la Commission.

Les personnes concernées recevront au moins un badge parmi les deux catégories suivantes: un badge personnel donnant accès aux locaux (badge d'accès) et, le cas échéant, un badge de fonction ne donnant pas accès aux locaux mais permettant l'identification du rôle spécifique de son détenteur:

1. badge d'accès (avec une présentation différente selon la catégorie de la personne concernée) – badge autorisant l'accès sur la base des droits d'accès spécifiques de la personne,
2. badge de fonction ou de rôle (avec une présentation différente selon le rôle de la personne concernée) – badge n'autorisant pas l'accès mais utilisé à des fins d'identification du rôle spécifique de la personne (p. ex. personnel de sécurité, personnel de sûreté, etc.)[2].

Selon la notification, les **champs de données** suivants seront traités (le cas échéant):

nom entier*; date de naissance*; photographie; nationalité*; numéro personnel (identifiant unique: numéro personnel pour le personnel de la Commission et numéro DB interne pour les autres personnes)*; sexe*; minuties des empreintes digitales; type de lien avec la Commission: fonctionnaire, agent temporaire, contractant, visiteur, agent contractuel, personnel retraité, membre de la famille d'un membre du personnel, etc.*; statut professionnel actuel: actif, détaché, absence de longue durée, etc.*; lieu de travail*; DG d'appartenance*; bureau et numéro(s) de téléphone/fax*; adresse électronique*; numéro de contrat et date d'expiration du contrat*; numéro et dates du document d'identité; droits d'accès; rôles associés aux privilèges et tâches système; données de contact de l'employeur pour les sous-traitants*; numéro de plaque minéralogique; données spécifiques relatives aux rôles au sein de la Commission: presse, représentation diplomatique, agent de sécurité, agent de sûreté, etc.*; informations sur la traversée du point d'accès: numéro de badge, date, heure, direction, alarmes et captures vidéo, le cas échéant, etc.; données relatives à l'exécution des tâches et aux opérations des gardes et patrouilles: présence ou inspection aux points de contrôle spécifiques, utilisation des dispositifs de sécurité (scanners) conforme aux exigences; images vidéo capturées par le système de vidéosurveillance associé[3].

---

[1] Les principales catégories sont les suivantes:

1. Personnel de la Commission (fonctionnaires ou personnel équivalent)
2. Personnel des organisations ou sociétés externes avec lesquelles la Commission a conclu des contrats spécifiques
3. Experts nationaux détachés (END; experts originaires d'États membres ou d'autres pays)
4. Personnel d'autres institutions ou organes européens
5. Visiteurs
6. Membres de la famille du personnel de la Commission
7. Personnel retraité de la Commission
8. Personnes accréditées (représentants de la presse et techniciens, représentants des États membres ou autres représentants diplomatiques ayant reçu une accréditation officielle des services de la Commission compétents)
9. Formateurs de la Commission
10. Autres – toute autre personne non comprise dans l'une des catégories susmentionnées et sollicitant l'accès aux locaux de la Commission.

[2] Les droits d'accès sont attribués sur la base de la catégorie de la personne concernée et de ses besoins en matière d'accès, tels que définis dans les politiques de sécurité de la Commission applicables en matière d'accès physique.

[3] Données suivies d'un astérisque: les données sont extraites de Sysper2/Comref pour le personnel de la Commission ou équivalent, d'ORIANA pour le personnel externe et d'e-Pass pour les visiteurs. Toutes les autres données sont générées ou collectées directement par le système.

Les champs de données ne sont pas tous traités ou conservés pour chaque personne concernée. Les champs traités ou enregistrés sont directement mis en rapport avec le type de lien qui unit la personne concernée à la Commission ou le motif de sa présence dans les locaux de la Commission.

Toutes les données susmentionnées peuvent être classées parmi les grandes catégories de données suivantes: données d'identification, données de transit, données relatives au matériel, données sur le profil de sécurité, données système et données de restriction.

1. Données d'identification: principalement des données relatives à l'identité et à la situation administrative de la personne concernée (y compris nom, numéro personnel, photographie, numéro de badge, numéro de téléphone, adresse du bureau, adresse électronique, numéro de la carte d'identité/passeport, minuties des empreintes digitales).
2. Données de transit: principalement des données relatives aux contrôles du dispositif de contrôle d'accès et aux événements/alarmes générés par l'utilisation du système par les personnes concernées (y compris numéro de badge, date/heure de la traversée des points de contrôle d'accès et du contrôle y associé, alarmes déclenchées par des incidents au cours de l'utilisation, badges présents dans une zone spécifique et fichiers vidéo).
3. Données relatives au matériel: principalement des données relatives au matériel de sécurité déployé (y compris noms des systèmes, adresses IP, emplacement et versions des logiciels).
4. Données sur le profil de sécurité: principalement des données sur la définition et la composition des groupes de sécurité, droits d'accès génériques et spécifiques, durées d'accès standard et non standard, durées d'accès autorisées, rôles dans le dispositif de sécurité.
5. Données système: principalement des données relatives à la gestion des systèmes (y compris utilisateur système et rôles définis, journaux système, pistes d'audit, heure d'accès pour les utilisateurs interactifs, le cas échéant).
6. Données de restriction: des données identifiant des personnes concernées auxquelles l'accès physique à une partie ou à l'ensemble des locaux de la Commission a été interdit pendant une certaine période. Cette liste contient uniquement les champs de données suivants: nom complet de la personne concernée, numéro d'identification (identifiant interne, numéro de carte d'identité ou tout autre numéro disponible), lieux interdits d'accès, date de début et de fin de l'interdiction.

L'enrôlement biométrique est réalisé sur une base volontaire et a pour principal objectif de faciliter l'accès aux locaux en dehors des heures de travail normales et aux zones sensibles ou à accès restreint (p. ex. les salles informatiques, les salles de configuration des communications). Dans certaines circonstances très spécifiques liées à des conditions de sécurité particulières (p. ex. niveaux d'alerte élevés, accès à des zones classées, etc.), la vérification biométrique peut être rendue obligatoire; elle sera mise en œuvre sur la base d'une évaluation au cas par cas.

Pour des motifs de résilience et de confort de l'utilisateur, deux doigts sont toujours utilisés pour l'enrôlement, de préférence un de chaque main. Il est proposé de prélever les empreintes des deux index ou des deux majeurs, mais le choix des doigts utilisés est laissé à l'utilisateur.

La procédure de vérification consiste essentiellement en un processus de vérification 1:1 (un à un) – les minuties intégrées dans la carte du détenteur étant comparées avec les minuties scannées (à des fins de vérification), sur place, à l'aide du lecteur/scanneur de données biométriques. La comparaison/vérification est effectuée localement par le lecteur de données biométriques – *lecteur à empreintes digitales.*

Les divers **destinataires** du traitement de données peuvent être classés au sein des catégories principales suivantes:
- les administrateurs du système (HR.DS.4[4]);
- les opérateurs du système (HR.DS.4);
- les opérateurs de la sécurité et de la sûreté (HR.DS.RA, HR.DS.1, HR.DS.2, HR.DS.4, HR.DS.6);
- les enquêteurs internes ou externes (enquêteurs officiels: HR.DS.RA, HR.DS.1, HR.IDOC, OLAF, CEPD, CJE);
- les gestionnaires des droits et profils d'accès;
- les validateurs (les personnes qui utilisent le système pour accéder aux locaux de la Commission)[5];
- la ou les applications informatiques (actuellement SYSPER: la photographie de la personne concernée peut être transférée à la demande de cette dernière);
- les responsables de la validation des requêtes (HR.DS.4, HR.DS.6, DG COMM, Chefs d'immeuble);
- les opérateurs locaux (LSO, etc.).

En ce qui concerne le **régime de conservation**, la notification mentionne que la politique de conservation suivante sera appliquée aux catégories de données définies ci-dessus:
1. données d'identification: conservation des données jusqu'à l'expiration du lien qui unit la personne concernée à la Commission + 6 mois; variable selon le type de lien (p. ex. membre du personnel: expiration du contrat + 6 mois, visiteur: fin de la visite + 6 mois, etc.);
2. données de transit: conservation des données fixée à 6 mois (y compris données vidéo, afin de permettre le lien avec les autres données de transit);
3. données sur les profils de sécurité: conservation illimitée des données (les données seront conservées aussi longtemps que nécessaire pour le bon fonctionnement du système)[6];
4. données système: conservation des données fixée à 1 an;

[4] Direction générale des ressources humaines et de la sécurité, direction Sécurité, Sécurité physique.

[5] La première version de la notification mentionnait les «utilisateurs finaux» parmi les destinataires. Ainsi que l'a précisé le responsable du traitement, dans le contexte de la notification, ces utilisateurs finaux sont à considérer comme des utilisateurs utilisant – ou interagissant avec – les interfaces informatiques du système en tant qu'utilisateurs finaux ordinaires. C'est le cas lors de la validation ou de la visualisation des demandes de visite par les utilisateurs internes. Ces utilisateurs ont accès aux données introduites par les visiteurs les concernant ou concernant leurs visites, raison pour laquelle ils sont désormais qualifiés de «validateurs».

[6] Les données sur les profils de sécurité ne semblent pas être des données à caractère personnel. Elles sont décrites essentiellement comme des ensembles de données sur les entrées, les périodes d'accès ou les autorisations d'accès requises par le système pour gérer les autorisations d'accès et les plannings. Une comparaison peut être établie avec les groupes d'accès et les autorisations associées définis dans les systèmes informatiques afin d'autoriser l'accès aux fichiers et aux ressources. Parmi les groupes classiques figurent:

a. ALL-BXL-BUILDINGS-Entrances – un groupe contenant toutes les principales entrées des bâtiments de Bruxelles;
b. ACCESS-24h-7d – un groupe autorisant l'accès à tout moment;
c. ACCESS-08-20-WeekDays – un groupe autorisant l'accès uniquement pendant les heures de travail normales;
d. Specific-Zone-ClassII – un groupe contenant tous les principaux points d'entrée (entrées) permettant d'accéder à la zone spécifique;
e. etc.

Ce sont des données système permanentes, raison pour laquelle aucune période de conservation n'est définie au préalable. Ces groupes sont conservés aussi longtemps que nécessaire (conservation quasi illimitée) après leur création. Lorsque des badges (identifiants) sont associés à ces groupes, la période de conservation normale s'applique aux données contenues dans le badge et aux données relatives à la personne concernée; si aucun badge n'est associé (groupe vide), il n'existe aucun lien avec des données à caractère personnel.

5. données de restriction (personnes inscrites sur une liste d'exclusion): la conservation des données est laissée à l'appréciation de l'autorité responsable de la Commission (à savoir l'autorité qui a décidé l'exclusion). Les données de cette catégorie sont totalement supprimées du système après autorisation adéquate de l'autorité responsable de la Commission.

Les données dont la période de conservation définie est dépassée seront:
1. copiées dans un autre système pour y être anonymisées et agrégées à des fins statistiques, si cela est jugé utile (entrepôt de données), ou
2. totalement supprimées des systèmes opérationnels informatiques.

Concernant l'anonymisation des données, elle fait globalement partie intégrante du processus en vertu de la procédure suivante:

a. chaque mois, le système d'entreposage des données se connecte à la base de données opérationnelle;
b. les séries de données (p. ex. production de badges, contrôles aux passages, personnes connues, etc.) pour lesquelles la période de conservation est dépassée sont sélectionnées;
c. les calculs requis pour l'agrégation (p. ex. le nombre de passages, le nombre de passages par jour/heure/mois, le nombre de refus d'accès, le nombre de refus de badge, le nombre de badges imprimés, etc.) des séries de données sélectionnées sont réalisés;
d. les valeurs calculées sont introduites dans le système d'entreposage des données;
e. au terme de ce processus, toutes les données sélectionnées (dont la période de conservation a expiré) sont supprimées de la base de données opérationnelle.

Les périodes et procédures de conservation des données s'appliquent à toute donnée collectée sur toute personne concernée qui accède ou s'enregistre pour accéder aux locaux de la Commission couverts par le système.

Cas particuliers:
1. Les données conservées dans les dispositifs de contrôle local des portes sont conservées pendant moins d'une semaine jusqu'à leur transfert vers le système centralisé ou leur écrasement par enregistrement de nouvelles données;
2. dans les stations de collecte, les images d'empreintes digitales et les minuties sont temporairement conservées dans un espace de mémoire ou de pagination. L'espace de stockage temporaire sera nettoyé au démarrage.
3. Les minuties des empreintes digitales (si utilisées) sont stockées sur la carte à puce RFID intégrée dans le badge de la personne concernée pour toute la durée de validité du badge (prévue pour dix ans).

Concernant les **droits** des personnes concernées, la notification indique que ces dernières sont informées de leurs droits, des points de contact disponibles, des voies et procédures de communication en place tels que décrits dans les documents et sources d'information précités.

Pour ce qui est des personnes inscrites sur la liste d'exclusion (données de restriction), elles sont informées de leurs droits par l'autorité de la Commission (direction Sécurité, IDOC ou service médical) responsable de l'exclusion. Sur ce point, le responsable du traitement de données relatives au contrôle d'accès ne dispose d'aucune information concernant les motifs ou la durée de l'exclusion d'une personne concernée et agit pour le compte de l'autorité de la Commission lorsqu'il traite ce type de données. Sur demande du directeur de la direction Sécurité, il met à jour la liste et active ou désactive les exclusions selon les instructions

reçues. Le CEPD souligne que cette procédure d'exclusion n'est pas couverte par la notification qui fait l'objet du présent avis.

Concernant les **informations** qui sont fournies, les documents suivants sont fournis:
- une brochure d'information spécifique (ou équivalent) destinée aux nouveaux détenteurs de badges est mise à leur disposition au moment de la remise du badge («Information des nouveaux détenteurs de badges»);
- une brochure d'information spécifique (ou équivalent) destinée aux visiteurs est mise à leur disposition aux réceptions des bâtiments («Information des visiteurs»);
- des panneaux d'information sont placés dans les zones de lecture des cartes à puce RFID, essentiellement à l'entrée des bâtiments, à des fins d'information (le contenu informatif présenté à l'annexe II du «Rapport sur les recommandations et les options technologiques du PSG» devrait y figurer);
- des panneaux d'information sont placés dans les zones d'enregistrement vidéo, essentiellement à l'entrée des bâtiments;
- sur l'intranet de la direction Sécurité, figurent des informations équivalentes à celles contenues dans la brochure susmentionnée destinée au nouveau personnel;
- sur le site Europa, figureront, lorsque des formulaires d'enregistrement en ligne généraux seront mis à disposition, des informations équivalentes à celles contenues dans la brochure susmentionnée destinée aux visiteurs;
- des informations et conseils appropriés sur les exigences en matière de traitement de données à caractère personnel seront mises en ligne sur la page d'accueil ou les pages pertinentes des interfaces web des utilisateurs/opérateurs du système spécifique en cours de déploiement;
- en cas de demande d'accès aux données des systèmes de contrôle d'accès physique, la personne est toujours informée dans le respect des règles qui régissent les demandes et par le service en charge de la demande.

Concernant le **stockage de données**, la notification décrit les règles suivantes.

Toutes les données opérationnelles ou actives seront stockées sur des serveurs groupés dédiés sur des espaces de stockage de données dédiés (disques). Les systèmes seront hébergés par les centres de données de la Commission.

Les données à caractère personnel seront cryptées avant tout transfert hors des principaux systèmes (p. ex. sauvegardes). Des sauvegardes seront effectuées vers les systèmes d'enregistrement centralisés dans les centres de données de la Commission.

Pour des raisons de planification de la continuité des activités et pour faire face aux éventuelles indisponibilités des serveurs centraux, une série de données cryptées sera copiée sur des serveurs dédiés hébergés dans la salle informatique de la direction Sécurité.

Le stockage provisoire de données sur des serveurs d'infrastructure est prévu à des fins de transmission ou de traitement temporaire. Il est essentiellement question de transmission de courrier électronique (saut de serveurs), de données collectées sur des sites externes avant leur transmission, de données introduites par des personnes concernées sur des bornes d'enregistrement et de délivrance de badges automatisés, de lecture optique de documents d'identité, etc.

Chaque dispositif de sécurité local (dispositif de contrôle des portes, boîtiers à clés, caméras IP, PC de contrôle ou de réception, etc.) utilisé pour la mise en œuvre du système de contrôle d'accès ou pour la surveillance contient une copie des autorisations d'accès requises

stockées sur son espace de stockage local. Ces dispositifs sont physiquement isolés et protégés de tout accès public. Seules les personnes autorisées peuvent traiter les données conservées.

Les minuties des empreintes digitales seront stockées exclusivement sur la carte à puce du badge de la personne concernée après l'enrôlement, lequel sera réalisé sur un système dédié. Lorsque les empreintes digitales sont utilisées aux fins du contrôle d'accès, une vérification (1:1) est réalisée au niveau du lecteur de badges en comparant le contenu du badge et l'empreinte qui vient d'être lue. Aucun stockage local ou central n'est effectué.

Diverses **mesures de sécurité** sont prévues dans la notification:

[...]

3. Analyse juridique

3.1. Contrôle préalable

Applicabilité du règlement n° 45/2001 («le règlement»): le présent avis relatif à un contrôle préalable porte sur le traitement de données à caractère personnel réalisé par la Commission européenne, en particulier la direction Sécurité.

Le règlement (CE) n° 45/2001 s'applique au *«traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier»* et au traitement *«par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire»*[7]. Pour les motifs décrits ci-après, tous les éléments qui donnent lieu à l'application du règlement sont présents.

Tout d'abord, des *données à caractère personnel* telles qu'elles sont définies à l'article 2, point a), du règlement (CE) n° 45/2001 sont collectées et traitées ultérieurement. Ensuite, les données à caractère personnel collectées sont soumises à un *«traitement automatisé»* au sens de l'article 2, point b), du règlement (CE) n° 45/2001, ainsi qu'à un traitement manuel. En effet, les données à caractère personnel telles que les données d'identification personnelle, dont les empreintes digitales, sont collectées et soumises à un «traitement automatisé», par exemple lorsque le service d'information prélève les empreintes. Enfin, le traitement est mis en œuvre par une institution, dans le cas présent la Commission européenne, pour l'exercice d'activités qui relèvent du champ d'application du droit de l'UE (article 3, paragraphe 1, du règlement).

Motifs de contrôle préalable: l'article 27, paragraphe 1, du règlement (CE) n° 45/2001 soumet au contrôle préalable du CEPD les *«traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités»*. Le CEPD estime[8] que la présence et le traitement de données biométriques autres que des photographies, comme c'est le cas dans la présente affaire étant donné que des empreintes digitales biométriques sont collectées, présentent des risques particuliers au regard des droits et libertés des personnes concernées. Il tire cette

[7] Voir l'article 3 du règlement (CE) n° 45/2001.

[8] Voir aussi les dossiers 2007-635 du 7 avril 2008 et 2008-223 du 30 juin 2008, disponibles sur le site du CEPD.

conclusion essentiellement de la nature des données biométriques, qui sont extrêmement sensibles, en raison de caractéristiques inhérentes à ce type de données. Par exemple, les données biométriques altèrent irrémédiablement la relation entre le corps et l'identité, en ce sens qu'elles rendent les caractéristiques du corps humain «lisibles à la machine» et susceptibles de faire l'objet d'une utilisation ultérieure. Ces risques justifient la nécessité de soumettre le traitement de données au contrôle préalable du CEPD afin de vérifier que des garanties strictes ont été mises en œuvre.

Par ailleurs, le CEPD estime que dans certains cas particuliers, l'intégration de la technologie RFID (carte à puce RFID intégrée dans le badge) dans le système de contrôle d'accès engendre des risques spécifiques. Par conséquent, le contrôle préalable en question est couvert par l'article 27, paragraphe 1, du règlement.

En outre, ainsi qu'il a déjà été mentionné précédemment, le CEPD considère que la procédure relative aux enquêtes ainsi qu'aux exclusions ne relève pas du champ d'application de la présente notification de contrôle préalable.

Délais: le contrôle préalable ayant pour objectif de répondre à des situations susceptibles de présenter des risques particuliers, l'avis du CEPD devrait être rendu avant le début du traitement. Le présent avis plaide en faveur de la réalisation d'un **contrôle préalable**. Dès lors, le traitement ne devrait pas être mis en œuvre tant que le CEPD n'a pas donné son approbation formelle.

La notification a été reçue le 3 juin 2010. En vertu de l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, la période de deux mois au cours de laquelle le CEPD doit rendre son avis a été suspendue pendant un total de 355 jours afin d'obtenir des informations supplémentaires ainsi que pendant la période relative au site de pré-production, auxquels s'ajoutent 39 jours afin de permettre la formulation de commentaires sur le projet d'avis. Le présent avis doit donc être adopté au plus tard le 13 septembre 2011.

3.2. Licéité du traitement

Le traitement de données à caractère personnel n'est autorisé que s'il est fondé sur l'article 5 du règlement (CE) n° 45/2001.

Parmi les divers motifs énoncés à l'article 5 du règlement (CE) n° 45/2001, celui qui s'applique au traitement notifié en vue d'un contrôle préalable est contenu à l'article 5, point a), aux termes duquel le traitement de données à caractère personnel ne peut être effectué que s'il est *«nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités […]»*. Interprétant l'article 5, point a), le considérant 27 établit que: *«(l)e traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes»*.

Afin de déterminer si le traitement est conforme à l'article 5, point a), du règlement (CE) n° 45/2001, trois éléments doivent être pris en compte: premièrement, si les traités ou d'autres actes législatifs prévoient le traitement effectué, deuxièmement, si le traitement est effectué dans l'intérêt public, et troisièmement, si le traitement est effectivement nécessaire à l'exécution de cette mission (test de nécessité). Les trois exigences sont étroitement liées.

* La **base juridique** applicable pour le traitement en question est à rechercher dans les actes suivants:

- la communication de la Commission sur le nouveau système d'accès et de sécurisation des immeubles de la Commission, C(2007)797 du 14 mars 2007;
- la décision de la Commission sur les tâches et responsabilités du Bureau de sécurité, C(94) 2129 du 8 septembre 1994;
- la responsabilité de la Commission sur la protection de son personnel (sécurité et sûreté) et de ses biens: décision 2007/65/CE de la Commission du 15 décembre 2006 sur les niveaux d'alerte et la gestion des situations de crise;
- les dispositions de la Commission en matière de sécurité: décision 2001/844/CE/CECA/Euratom de la Commission du 29 novembre 2001 modifiant son règlement intérieur.

* Le traitement est réalisé dans le cadre de **l'exercice légitime de l'autorité publique**. Le CEPD constate que la Commission réalise les activités de traitement dans le cadre d'une mission relevant de l'exercice légitime de son autorité publique sur la base des actes législatifs susmentionnés adoptés sur la base du statut des fonctionnaires.

* Concernant la nécessité du traitement **(test de nécessité)**, conformément à l'article 5, point a), du règlement (CE) n° 45/2001, le traitement de données doit être *«nécessaire à l'exécution d'une mission»* tel que mentionné plus haut. À cet égard, le considérant 27 établit que *«(l)e traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes»*.

Sous ce rapport, le traitement concerné a pour finalité la protection physique du personnel, des informations et des biens de la Commission, l'établissement de conditions de sûreté pour le personnel travaillant sur le site (y compris pour les cas d'évacuation et les situations de crise) et les visiteurs, et le contrôle de l'accès à la propriété de la Commission.

Au vu de l'importance de ces intérêts, la Commission européenne pourrait effectivement juger nécessaire d'adopter des mesures de sécurité spéciales, notamment la mise en place de systèmes de contrôle d'accès rigoureux, et d'autoriser l'IDOC et l'OLAF à mener des enquêtes sur les incidents de sécurité.

Par conséquent, le CEPD est d'avis qu'il est raisonnable de considérer que, dans le cas présent, la mise en œuvre de systèmes de contrôle d'accès rigoureux donnant lieu au traitement de données à caractère personnel est une mesure de contrôle interne nécessaire en vue de la protection des données et des intérêts de l'UE.

3.3. Qualité des données

Adéquation, pertinence et proportionnalité: en vertu de l'article 4, paragraphe 1, point c), du règlement (CE) n° 45/2001, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Il s'agit du principe de qualité des données.

Le CEPD a analysé les champs de données qui seront traités (le cas échéant) et en conclut que la liste actuelle de champs de données est compatible avec le règlement (CE) n° 45/2001. Il est par ailleurs précisé que les champs de données ne sont pas tous traités ou conservés pour

chaque personne concernée. Les champs traités ou enregistrés sont directement mis en rapport avec le type de lien qui unit la personne concernée à la Commission ou avec le motif de sa présence dans les locaux de la Commission.

Concernant les données biométriques, le CEPD note que seules les personnes qui ont besoin d'un accès spécial seront enrôlées dans le système et seront dès lors soumises au prélèvement de leurs empreintes digitales. En outre, pour des motifs de résilience et de confort de l'utilisateur, deux doigts sont toujours utilisés pour l'enrôlement, de préférence un de chaque main. Il est proposé de prélever les empreintes des deux index ou des deux majeurs, mais le choix des doigts utilisés est laissé à l'utilisateur. Le type de données collectées, essentiellement les relevés des empreintes digitales de deux doigts et des informations d'identification connexes, correspond aux données requises pour l'exploitation d'un système de contrôle d'accès sur la base de données biométriques. De ce point de vue, le CEPD souligne que les données collectées pourraient être jugées adéquates et pertinentes aux fins du traitement.

Utiliser la vérification des minuties des empreintes digitales comme méthode de validation des données biométriques pourrait être jugé adéquat.

La procédure de vérification consiste essentiellement en un processus de vérification 1:1 (un à un) – les minuties intégrées dans la carte du détenteur étant comparées avec les minuties scannées (à des fins de vérification), sur place, à l'aide du lecteur/scanneur de données biométriques. La comparaison/vérification est effectuée localement par le lecteur de données biométriques – *lecteur à empreintes digitales.* Le CEPD estime cette vérification plus respectueuse de la vie privée qu'une comparaison avec des données de référence contenues dans une base de données.

Loyauté et licéité: l'article 4, paragraphe 1, point a), du règlement requiert que les données soient traitées loyalement et licitement. La question de la licéité a été analysée plus haut (voir le point 2.2.2), tandis que celle de la loyauté est étroitement liée à la question de l'information des personnes concernées, traitée ci-après au point 2.2.9.

Exactitude: selon l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel doivent être *«exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées»*.

En l'espèce, les données à caractère personnel concernées par le traitement comprennent des données biométriques, utilisées à des fins de contrôle d'accès. Certaines caractéristiques clés des systèmes biométriques ont un impact direct sur le niveau d'exactitude des données générées aux cours des phases d'enrôlement ou d'identification inhérentes à ce type de système. Selon que le système biométrique est établi d'une manière qui intègre ces éléments clés ou non, l'exactitude des données constituera (ou non) un paramètre à prendre en compte. Le CEPD a analysé, dans des avis précédents relatifs au contrôle d'accès, les règles à suivre lors de la mise en œuvre de systèmes biométriques[9]. L'analyse suivante décrit ces éléments clés et évalue dans quelle mesure ils ont été pris en considération dans le système de contrôle d'accès informatique fondé sur des données biométriques concerné.

[9] Voir par exemple les dossiers 2007-0635 et 2008-0223 sur le contrôle d'accès à l'OLAF (physique et logique).

Premièrement, toute phase d'enrôlement doit prévoir des moyens d'identification alternatifs des personnes qui ne sont pas éligibles, même temporairement, à la procédure d'enrôlement, par exemple en raison d'empreintes digitales endommagées. Cette procédure est généralement qualifiée de ***«procédure de secours»***[10].

En ce qui concerne la phase d'enrôlement en tant que telle, le responsable du traitement a décidé, à la suite de la phase de pré-production, d'inclure dans la procédure d'enrôlement une vérification de chaque empreinte digitale prélevée avant la finalisation et la délivrance des badges afin de réduire les risques de rejets ultérieurs – *faux rejets*. Selon la Commission, cette étape de vérification associée à des indicateurs de qualité du scannage des doigts, fournis par tout logiciel d'enrôlement professionnel, crée les conditions nécessaires pour réduire au minimum le risque de refus ultérieur.

En outre, à la suite de la phase de pré-production, si des données biométriques ne sont pas disponibles ou si la vérification biométrique n'est pas possible, à un moment de vérification spécifique, la ou les *solutions de secours* suivantes seront déployées selon la situation rencontrée et les conditions particulières de vérification du contrôle d'accès en vigueur:

1. la reconnaissance faciale du détenteur du badge par une personne de confiance (p. ex l'opérateur de la salle de contrôle, du personnel de sécurité, une personne responsable de la zone, etc.), à distance ou sur place, aux fins d'autoriser l'accès;
2. pour l'accès à des zones moins sensibles, l'utilisation d'un code PIN secret peut être proposée en lieu et place de la vérification des minuties des empreintes digitales biométriques.

Le CEPD juge ces procédures de secours satisfaisantes, mais rappelle à la Commission que ces mesures doivent prendre en considération le niveau de risque pour la sécurité du bâtiment et devraient également protéger les droits de la ou des personnes concernées.

En outre, dans le cas d'un faux rejet, le CEPD suggère à la Commission de mettre au point une procédure visant à résoudre le problème sans lourdeurs excessives pour les personnes, en d'autres termes, une procédure alternative qui offre des solutions suffisamment simples au problème de non-identification et de rejet. Le CEPD souhaiterait, à cet égard, que la Commission prévoie un renouvellement périodique des prélèvements afin de maintenir un haut niveau de qualité des données. L'établissement d'une fréquence de renouvellement se justifie notamment en raison du fait que les données biométriques, en particulier les empreintes digitales, peuvent évoluer au cours de la vie d'une personne concernée. Elle est également justifiée par l'éventuelle altération, au fil du temps, de l'épiderme du doigt choisi pour le prélèvement, ainsi que par la qualité du gabarit de l'empreinte enregistré pendant l'enrôlement. Cette fréquence de renouvellement pourrait être définie et appliquée au terme de deux années d'exploitation du nouveau système, sur la base de l'expérience du système acquise par la Commission.

Enfin, les minuties seront stockées uniquement dans la mémoire interne de la carte à puce, ainsi qu'il a été annoncé, et le processus de vérification – comparaison des minuties, vérification 1:1 – sera exécuté sur place par le lecteur de données biométriques. Le CEPD est

[10] Pour une description des principes de protection des données applicables dans le cadre des procédures de secours, voir l'avis du Contrôleur européen de la protection des données sur le projet de règlement du Conseil (CE) portant fixation de la forme des laissez-passer délivrés aux membres et aux agents des institutions, JO C 313 du 20.12.2006, p. 36.

favorable à ce système, qui empêche toute utilisation ultérieure illicite et attaque de hameçonnage qui sont généralement le corollaire de l'utilisation de bases de données[11].

3.4. Conservation des données

En vertu de l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Ce principe est communément appelé «principe de conservation».

La Commission déclare que la période de conservation prévue en ce qui concerne les données d'identification est de six mois et que celle prévue pour les données système est d'un an:

- concernant les données d'identification, le CEPD note que la durée établie à la lumière de l'article 4 du règlement susmentionné, aussi longue que les périodes de conservation prévues pour les différentes catégories de données, pourrait être jugée justifiée;

- concernant la conservation des données système, le CEPD suppose que ces données représentent les journaux d'accès. Il estime, à cet égard, que la Commission européenne devrait, un an après le lancement du système, évaluer la nécessité de conserver les données pendant cette durée et adapter la période de conservation si nécessaire. Dans d'autres dossiers examinés[12], le CEPD a estimé qu'une période de conservation de trois mois pouvait être considérée comme raisonnable.

En outre, les minuties des empreintes digitales (si utilisées) sont conservées à titre permanent dans la carte à puce RFID intégrée dans le badge de la personne concernée, et ce pour toute la durée de validité du badge (prévue pour dix ans). Le CEPD juge cette durée de conservation appropriée.

3.5. Transfert de données

Selon la notification et le document «Destinataires du traitement», divers destinataires au sein de la DG HR DS peuvent avoir accès aux données. Les enquêteurs, internes ou externes, de la DG HR DS peuvent également y avoir accès dans le cadre de leurs enquêtes (IDOC, OLAF, CEPD, CJE).

Le CEPD rappelle que l'article 7 du règlement (CE) n° 45/2001 autorise les transferts de données à caractère personnel s'ils sont *«nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire»*. Aux fins du respect de cette disposition, lors du transfert de données à caractère personnel, le HR DS doit s'assurer que i) le destinataire possède les compétences appropriées et que ii) le transfert est nécessaire. Le CEPD estime que ces conditions sont respectées lors de la notification d'incidents de sécurité dans ce cas-ci. Cependant, la légitimité d'un transfert au regard de ces critères devra être évaluée au cas par cas. Outre ce qui précède, il convient, aux fins de l'article 7 du règlement, d'informer le destinataire de la nécessité de traiter les données à caractère personnel uniquement aux fins qui ont motivé leur transmission.

[11] Voir l'avis sur une notification de contrôle préalable reçue du délégué à la protection des données de la Banque centrale européenne concernant l'intégration dans un système de contrôle d'accès préexistant d'une technologie d'analyse de l'iris pour les zones hautement sécurisées de la BCE, 14 février 2008 (2007-501), disponible sur le site du CEPD.

[12] Voir les dossiers de l'OLAF précités.

Aucun autre transfert au titre des articles 8 et 9 n'est prévu. Toutefois, il se peut qu'il faille divulguer des données aux forces de l'ordre nationales, dans le cadre d'activités de prévention de la criminalité ou d'enquêtes. Dans pareil cas, le CEPD souligne qu'en vertu de l'article 8 du règlement, les données à caractère personnel ne sont transférées que si *«a) le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique, ou b) le destinataire démontre la nécessité de leur transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes de la personne concernée».*

Le CEPD rappelle à la Commission qu'il conviendrait de réaliser une telle analyse au cas par cas.

Enfin, au vu des informations fournies, aucun transfert n'est effectué vers des pays tiers.

3.6. Traitement du numéro personnel ou de l'identifiant unique

L'article 10, paragraphe 6, du règlement prévoit que *«(l)e contrôleur européen de la protection des données détermine les conditions dans lesquelles un numéro personnel ou tout autre identifiant utilisé de manière générale peut faire l'objet d'un traitement par une institution ou un organe communautaire»*. Le présent avis n'établira pas les conditions générales de l'utilisation d'un numéro personnel, mais envisagera les mesures spécifiques nécessaires dans le contexte du PACS.

Le CEPD a d'ores et déjà précisé, dans un précédent avis de contrôle préalable[13], le statut d'un numéro de carte à puce intégrée dans une carte. Le numéro d'identification associé à la carte à puce RFID fait partie des données à caractère personnel couvertes par le règlement n° 45/2001. En effet, ce numéro d'identification, lorsqu'il est utilisé pour évaluer le comportement d'un membre du personnel et qu'il est lié au numéro personnel (au nom d'une personne, comme c'est le cas dans le présent dossier), donne lieu à un traitement de données à caractère personnel, nécessitant dès lors le respect des principes de protection des données.

L'utilisation du numéro personnel est nécessaire parce que l'identifiant de la carte est communiqué au système de contrôle d'accès. Dans le cas présent, l'utilisation du numéro personnel des membres du personnel aux fins de la vérification des données relatives au droit d'accès dans le système est raisonnable si l'on considère que ce numéro est utilisé pour identifier la personne dans le système et permet ainsi de garantir l'exactitude des données.

3.7. Droit d'accès et de rectification

Aux termes de l'article 13 du règlement (CE) n° 45/2001, *«(l)a personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, du responsable du traitement (…) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données»*. L'article 14 garantit aux personnes concernées le droit de rectifier des données inexactes ou incomplètes.

[13] Voir l'avis sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de la «mise en œuvre du Flexitime spécifique à la DG INFSO», 19 octobre 2007 (2007-218).

La notification précise que les personnes concernées sont informées de leurs droits, des points de contact disponibles, des voies et procédures de communication en place tels que décrits dans les documents et sources d'information précités (voir le point 2 de la section «Faits»). En outre, sur la base des informations fournies, la Commission européenne semble dûment respecter les droits des personnes concernées, conformément au règlement (CE) n° 45/2001.

Le responsable du traitement a également transmis au CEPD le document relatif au délai établi dans le cadre du PSG pour le verrouillage/effacement des données, et aux catégories de données définies. Ce document présente les catégories de données prévues et détaille la politique générale de verrouillage/effacement de données sur demande légitime et motivée des personnes concernées.

Dans les cas où l'article 20 s'appliquerait (p. ex. dans le cas d'enquêtes), le CEPD rappelle à la Commission qu'il convient de l'appliquer de manière restrictive et au cas par cas.

En conclusion, le CEPD estime que les conditions visées aux articles 13 et 14 du règlement sont remplies moyennant une application au cas par cas.

3.8. Information des personnes concernées

En vertu des articles 11 et 12 du règlement (CE) n° 45/2001, les responsables de la collecte des données à caractère personnel doivent informer les personnes de la collecte de leurs données. Par ailleurs, ces personnes sont en droit d'être informées, notamment, des finalités du traitement, des destinataires des données et de leurs droits spécifiques en tant que personnes concernées.

La Commission européenne a transmis au CEPD la déclaration de confidentialité destinée aux personnes concernées qui utiliseront le PACS. Cette déclaration de confidentialité est mise en ligne sur l'intranet et sera distribuée aux détenteurs des nouveaux badges.

Le CEPD a également réexaminé le contenu des informations fournies dans la déclaration de confidentialité afin de vérifier s'il satisfaisait aux exigences des articles 11 et 12 du règlement (CE) n° 45/2001.

Il en a conclu que les éléments prévus aux articles 11 et 12 du règlement (CE) n° 45/2001 y étaient présents.

3.9. Mesures de sécurité

Conformément à l'article 22 du règlement, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger. Ces mesures sont prises notamment afin d'empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite.

[...]

La notification indique par ailleurs qu'une évaluation complète des risques informatiques sera réalisée et que les contrôles de sécurité et les mesures d'atténuation des risques appropriés seront mis en œuvre. Elle prévoit également que tout risque résiduel sera documenté et

formellement accepté par le responsable du traitement et le sous-traitant. Le CEPD souhaite avoir accès aux résultats de l'évaluation des risques.

Au vu des informations disponibles, le CEPD estime qu'il n'y a pas lieu de penser que la Commission européenne n'a pas appliqué les mesures de sécurité prévues à l'article 22 du règlement, mais l'invite à lui transmettre les documents précités.

Conclusion:

Le traitement proposé ne paraît pas entraîner de violation des dispositions du règlement (CE) n° 45/2001 pour autant que la Commission européenne:

- évalue la pertinence de la durée de conservation des données système et l'adapte un an après la mise en service du PACS;

- autorise le CEPD à accéder aux résultats de l'évaluation des risques informatiques réalisée et à la liste des contrôles de sécurité et des mesures d'atténuation mis en œuvre;

- fournisse au CEPD la documentation relative à la procédure établie en cas d'incidents de sécurité.

Fait à Bruxelles, le 8 septembre 2011

(**signé**)

GIOVANNI BUTTARELLI
Contrôleur européen adjoint de la protection des données