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 l'autorisation d'entrée et du contrôle des accès pour la protection physique au Centre commun de recherche ITU

Bruxelles, le 24 juillet 2012 (dossier 2008-0726)

I. Procédure

Le 28 novembre 2008, le contrôleur européen de la protection des données (ci-après «le CEPD») a reçu du délégué à la protection des données (ci-après «le DPD») de la Commission européenne une notification en vue d'un contrôle préalable (ci-après «la notification») à propos des opérations de traitement de données en relation avec le fonctionnement d'une autorisation d'entrée et d'un contrôle des accès pour la protection physique au Centre commun de recherche – Institut des transuraniens, situé à Karlsruhe (ci-après «le CCR-ITU»).

Le 26 janvier 2009, le CEPD a demandé des informations complémentaires, que le DPD lui a envoyées le 20 février 2009. Les informations complémentaires ont rendu l'affaire plus complexe, nécessitant une analyse plus approfondie du dossier. Pour cette raison, le CEPD a décidé le 23 février 2008 de prolonger de 3 semaines supplémentaires la période d'analyse complémentaire. Une deuxième demande d'informations, ainsi que le projet d'exposé des faits, ont été envoyés au DPD de la Commission le 4 mars 2009. Le 9 avril 2009, le CEPD a demandé un retour d'information quant à deux questions supplémentaires.
Le CEPD a reçu les réponses le 4 mai 2009.

Le 11 mai 2009, le CEPD a envoyé le projet d'avis au DPD de la Commission afin qu'il formule ses observations. Des rappels ont été envoyés au DPD de la Commission le 5 décembre 2011 et le 26 juin 2012. Les observations sur le projet d'avis n'ont pas été transmises au CEPD.

II. Les faits

Le système d'autorisation d'entrée et de contrôle des accès pour la protection physique (ci-après «le système AECAPP») fait partie des infrastructures de sécurité du CCR-ITU et est destiné à contrôler et gérer les droits d'accès aux locaux du CCR-ITU. En outre, l'AECAPP assiste également le service de radioprotection au sein du CCR-ITU afin de contrôler le statut de radioprotection des visiteurs. Le présent contrôle préalable analysera le traitement des données pour la première finalité. Il ne s'intéressera toutefois pas aux questions de protection des données liées à la finalité secondaire dans la mesure où le CEPD a déjà mené un contrôle

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

préalable des opérations de traitement conduites quant à l'exposition personnelle aux radiations selon les mesures dosimétriques[1].

Dans ce contexte, il est important de tenir compte de l'intérêt public éminent à la sécurité et à la sûreté des activités sous-jacentes motivant le traitement des données. En même temps, il est important que lesdites activités de sécurité et de sûreté soient menées sans mettre en péril la protection des données et des droits au respect de la vie privée.

La ***finalité*** du système AECAPP est double: *(i)* contrôler et gérer les droits d'accès au CCR-ITU. Cela s'applique à l'ensemble du site du CCR-ITU dans la mesure où l'ensemble du CCR-ITU est réputé constituer une installation nucléaire, *(ii)* contrôler le statut de radioprotection.

Le traitement des données relève de la ***responsabilité première*** du CCR-ITU, en particulier de l'unité compétente pour la sécurité nucléaire (unité E07), qui représente le responsable du traitement («le CCR-ITU») pour le traitement en cause. Deux sous-traitants sont utilisés, l'un pour accomplir les tâches de protection physique (désigné «groupe de protection physique») et un autre pour entretenir et développer le logiciel et le matériel utilisés pour le traitement des données.

Pour ce qui est de la ***description de la manière dont le traitement est réalisé***, les éléments pertinents sont présentés ci-après.

<u>Concernant le traitement des données des visiteurs et des fournisseurs à court terme:</u>

(i) *Phase d'enrôlement:* pendant cette phase, les visiteurs et les fournisseurs à court terme remplissent un formulaire (ci-après le «formulaire de demande») en donnant des informations sur leur identité, leur lieu de naissance, leur nationalité, leur numéro de passeport, leur adresse privée et leur employeur. En outre, la personne accueillie remplit un formulaire de demande où elle donne des informations sur la durée de son séjour, sur la nécessité d'accéder à des zones contrôlées, sur le motif de son séjour et sur la ou les personne(s) à laquelle ou auxquelles elle rend visite. Ces informations sont transmises à la DG ADMIN DS en vue de la délivrance d'une habilitation de sécurité (voir ci-dessous).

(ii) *Délivrance d'un badge:* à la suite de l'analyse du formulaire de demande et après l'obtention de l'habilitation de sécurité, un badge comportant les droits d'accès autorisés est délivré par le personnel du groupe de protection physique. Le badge comporte le prénom et le nom, le numéro de badge et une photographie afin de pouvoir identifier à tout moment la personne et ses droits d'accès aux différentes zones de sécurité.

(iii) *Utilisation du badge:* à chaque fois qu'un titulaire du badge souhaite accéder à une zone de sécurité, une vérification de son identité et de ses droits d'accès est réalisée par le groupe de protection physique, c'est-à-dire par des gardes accomplissant des missions de protection physique.

(iv) *Conservation des données:* toutes les données seront saisies dans la base de données centrale ZES du groupe de protection physique.

[1] 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 base de données AGS-EDV du Centre commun de recherche ITU, situé à Karlsruhe, Bruxelles, 10 janvier 2008 (dossier 2007-378).

Concernant le traitement des données du personnel de la Commission et des fournisseurs à long terme de l'ITU (dans l'ensemble, du personnel de l'ITU) ayant besoin d'accéder quotidiennement aux zones nucléaires ou aux autres zones de sécurité:

Le personnel de l'ITU fait l'objet du traitement décrit ci-dessus au moment où il commence à travailler pour l'ITU. En outre, un traitement supplémentaire est réalisé, impliquant une numérisation [biométrique]:

(i) *Phase d'enrôlement:* pendant cette phase [un appareil photographique] prend des clichés en noir et blanc des [données biométriques] du personnel de l'ITU (désignées «codes [...]»). Cela est réalisé par des opérateurs ayant suivi une formation spécifique sur les procédures d'enrôlement biométrique. Le groupe de protection physique y procède au bureau des demandes situé dans les locaux de l'ITU et constituant une des zones de sécurité à accès limité. En cas de «faux rejet», il est prévu qu'il soit procédé à une vérification manuelle après une identification des gardes.

Tout le personnel de l'ITU (c'est-à-dire le personnel de la Commission et les fournisseurs à long terme) est enrôlé dans la mesure où la totalité du site du CCR-ITU constitue une installation nucléaire. Les membres du personnel de l'ITU concernés sont approximativement au nombre de 400.

(ii) *Conservation des [données biométriques]:* les images des [données biométriques] sont conservées dans une base de données des codes [...]. Les données d'identification, comme indiqué plus haut, sont conservées dans une base de données centrale ZES. Cette mesure est destinée à garantir que le «code [...]» ne soit utilisable que par une personne ayant accès aux deux bases de données à la fois. L'accès aux deux bases de données est limité au groupe de protection physique.

(iii) *Numérisation des [données biométriques]:* [...] en l'occurrence, l'AECAPP du CCR-ITU utilise un mode de recherche par comparaison avec un grand nombre (*«one-to-many»*). En plus de la vérification des [données biométriques], les personnes sont pesées afin qu'une seule personne autorisée à la fois passe la porte. En cas de faux rejet, il est prévu que les gardes procèdent à une vérification et une identification manuelles.

Le serveur de la base de données centrale constitue l'interface administrative avec le système. Il conserve les informations concernant les utilisateurs et leurs droits d'accès. Il garde également la trace de toutes les tentatives d'accès, fructueuses ou non.

Les ***personnes concernées*** incluent les membres du personnel de l'ITU et les fournisseurs à long terme. En outre, les données des visiteurs et des fournisseurs à court terme seront également traitées dans le contexte de la délivrance de cartes temporaires.

Les ***catégories de données à caractère personnel*** suivantes sont concernées: (i) données d'identification (nom, numéro personnel, photographie, date et lieu de naissance, nationalité, adresse privée); (ii) informations relatives au travail (nom de la société, début et fin du travail au CCR-ITU); (iii) informations relatives à l'habilitation de sécurité; (iv) droits d'accès et données d'enregistrement (date, heure, accès accordé ou refusé) et (v) informations sur la protection contre les radiations (formation, exposition professionnelle).

Certaines informations sont ***transférées*** à la DG ADMIN DS. Tout visiteur de pays hors de l'UE souhaitant avoir accès aux locaux de l'ITU doit être habilité par la DG ADMIN DS. À cette fin, des informations telles que la date et le lieu de naissance, la nationalité, le numéro

d'identification personnel, l'adresse privée, la société et l'objet de la visite sont transmises à la DG ADMIN DS. En cas d'incident de sécurité, des informations peuvent être partagées avec les autorités nationales compétentes allemandes.

Concernant l'utilisation d'un ***sous-traitant***, il s'agit en l'espèce du groupe de protection physique et d'une société privée chargée d'entretenir et de développer le logiciel et le matériel utilisés pour le traitement des données. Le CEPD constate que des contrats de sous-traitance sont en place et garantissent que les sous-traitants prennent les mesures de sécurité adéquates pour protéger les informations.

Concernant les ***informations données aux personnes concernées***, selon la notification une déclaration de confidentialité sera disponible sur l'intranet du CCR-ITU et au poste de garde à l'entrée des locaux de l'ITU. La déclaration de confidentialité comprend les éléments suivants: (i) une explication du système d'autorisation d'entrée et de contrôle des accès de l'ITU; (ii) les informations à caractère personnel collectées, la fin à laquelle ces informations sont collectées et les moyens techniques utilisés pour cette collecte; (iii) les modalités de protection des informations; (iv) la durée de conservation des données; (v) la présentation des droits des personnes concernées (en termes d'accès, de modification et de suppression) et la mention du droit de saisir le CEPD. Le DPD a joint un projet de déclaration de confidentialité à la notification. Les droits des personnes concernées sont expliqués dans la déclaration de confidentialité et des coordonnées sont fournies afin que les personnes concernées puissent exercer leurs droits.

Concernant la ***conservation des données***, selon la notification et la déclaration de conformité, les données des visiteurs n'ayant pas accès à une zone nucléaire proprement dite sont conservées pendant 5 ans après la dernière visite. Pour le personnel du CCR-ITU, les données seront détruites 5 ans après la date d'expiration de l'habilitation de sécurité. La raison de la conservation de ces informations pendant cette durée est la suivante: les visiteurs sont pour la plupart des techniciens spécialisés ou des scientifiques de haut niveau qui visitent régulièrement le CCR- ITU, généralement pendant plusieurs années. Par conséquent, le CCR-ITU a décidé de conserver les données pendant 5 ans afin de pouvoir demander le renouvellement des habilitations de sécurité sans devoir collecter les données des personnes à chaque fois qu'elles visitent le CCR-ITU.

Pour les visiteurs et le personnel de l'ITU ayant accès aux zones nucléaires proprement dites et dont les données de dosimétrie sont enregistrées, les données seront conservées pendant 95 ans après la date de naissance de la personne concernée. Cela s'applique à toutes les données à l'exception des codes [...]. Elles sont conservées afin de pouvoir retrouver tout incident ou tout élément relatif aux valeurs de dosimétrie et pour pouvoir identifier et contacter la personne en question.

Des ***mesures de sécurité*** sont appliquées. Les informations sont conservées sur des systèmes informatiques sécurisés, hébergés et gérés par le groupe de protection physique. L'accès au système de la base de données requiert la saisie d'un identifiant utilisateur et d'un mot de passe. Les données sont automatiquement sauvegardées sur bande. Toutes les informations sur papier sont conservées dans des zones sécurisées.

III. Aspects juridiques

III.1. Contrôle préalable

Le présent avis en vue d'un contrôle préalable porte sur le traitement d'informations à caractère personnel auquel procède le CCR-ITU pour contrôler l'identité des personnes entrant et sortant du CCR-ITU et leur autoriser ou refuser l'accès.

Le règlement (CE) n° 45/2001[2] 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 dans un fichier»* et au traitement *«par toutes les institutions et 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»*[3]. Pour les raisons exposées ci-après, tous les éléments justifiant l'application du règlement sont réunis en l'espèce.

Premièrement, les données à caractère personnel telles que définies à l'article 2, point a), du règlement (CE) n° 45/2001 sont collectées et traitées ultérieurement. Deuxièmement, les données à caractère personnel collectées font l'objet de *«traitements automatisés»*, tels que définis à l'article 2, point b), du règlement (CE) n° 45/2001, ainsi que de traitements manuels. En effet, les données à caractère personnel, telles que les données [biométriques], sont collectées et font l'objet d'un traitement automatisé, par exemple lorsque des modèles [biométriques] sont établis. Enfin, le traitement est effectué par un organe communautaire, ici le CCR-ITU à Karlsruhe, dans le cadre du droit de l'Union [article 3, paragraphe 1, du règlement (CE) n° 45/2001]. Par conséquent, tous les éléments justifiant l'application du règlement sont réunis en l'espèce.

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 que la présence de certaines données biométriques, comme c'est le cas en l'espèce, où des [...] biométriques sont collectées, présente des risques particuliers au regard des droits et libertés des personnes concernées. Ce point de vue se fonde principalement sur la nature des données biométriques, qui sont extrêmement sensibles en raison de certaines des caractéristiques qui leur sont inhérentes. Ainsi, les données biométriques modifient irrévocablement la relation entre le corps et l'identité en ce sens qu'elles rendent les caractéristiques du corps humain lisibles par une machine et susceptibles d'être utilisées ultérieurement. En outre, concernant ces données, le CEPD note également les possibilités d'interconnexions et la situation actuelle en termes d'outils technologiques, qui peuvent avoir des conséquences inattendues et/ou fâcheuses pour les personnes en question. Ces risques justifient la nécessité de soumettre le traitement des données à un contrôle préalable du CEPD afin de vérifier que des mesures adéquates de protection des données et de la vie privée adéquates ont été mises en œuvre.

***Contrôle préalable effectué* a posteriori**. Le contrôle préalable ayant pour objet d'étudier les situations susceptibles de présenter certains risques, l'avis du CEPD devrait être rendu avant le début du traitement. Or, en l'espèce, le traitement a déjà commencé. En tout état de cause, il ne s'agit pas d'un problème insurmontable si toutes les recommandations du CEPD sont pleinement prises en compte et que le traitement est ajusté en conséquence.

Notification et date d'échéance pour l'avis du CEPD. La notification a été reçue le 28 novembre 2008. Le délai durant lequel le CEPD doit rendre son avis a été étendu de trois

[2] Règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après dénommé «le règlement (CE) n° 45/2001»).
[3] Voir l'article 3 du règlement (CE) n° 45/2001.

semaines. Le délai durant lequel le CEPD doit rendre son avis a été suspendu pour un total de 1 256 jours afin d'obtenir des informations supplémentaires du CCR-ITU et pour permettre la formulation des observations sur le projet d'avis du CEPD.

III.2. Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que s'il est justifié par des motifs visés à l'article 5 du règlement (CE) n° 45/2001.

Parmi les différents motifs énumérés à l'article 5 du règlement (CE) n° 45/2001, le traitement notifié en vue d'un contrôle préalable relève de l'article 5, point a), qui prévoit que le traitement de données peut être effectué 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 ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe communautaire ou le tiers auquel les données sont communiquées»*.

Afin de déterminer si le traitement est conforme à l'article 5, point a), du règlement (CE) n° 45/2001, il convient de répondre aux trois questions ci-après.

Premièrement, le traité ou d'autres actes législatifs prévoient-ils ce traitement de données («base juridique»)? Le CEPD considère que la ***base juridique*** du traitement comprend:

- la décision 2001/844/CE, CECA, Euratom de la Commission (dispositions en matière de sécurité);
- la décision 2006/3602/CE de la Commission concernant la sécurité des systèmes d'information;
- la politique de la Commission en matière de sécurité des systèmes d'information (PolSec);
- la législation allemande comprenant (i) Atomgesetz (AtG) §9+§12b+§12c du 15 juillet 1985, (ii) Atomrechtliche Zuverlässigkeitsüberprüfungsverordnung (AtZüV) du 1er juillet 1999 http://www.gesetze-im-internet.de/atz_v/index.html, (iii) Strahlenschutzverordnung (StrlSchV) §42 du 20 juillet 2001.

Deuxièmement, le traitement est-il effectué dans l'intérêt public? Le CEPD note que la mission du CCR-ITU est d'apporter une base scientifique à la protection des citoyens européens contre les risques associés au traitement et au stockage de matières hautement radioactives. La Commission met en œuvre le traitement dans l'exercice légitime de son autorité publique et à la lumière de l'intérêt public exigeant que cette recherche soit menée de manière adéquate et sûre.

Finalement, le traitement est-il effectivement nécessaire à l'exécution de cette mission («critère de la nécessité»)? Selon l'article 5, point a), du règlement (CE) n° 45/2001, le traitement des données doit être «nécessaire à l'exécution d'une mission», comme indiqué ci-dessus. À cet égard, le considérant 27 du règlement précise que *«le 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»*. Compte tenu du caractère extrêmement sensible de la finalité et des informations traitées au sein du CCR-ITU, et pour prévenir l'accès non autorisé et la divulgation de ces informations sensibles, il convient que le CCR-ITU mette en œuvre des mesures extrêmement sûres pour contrôler l'accès à ses locaux. Ces mesures incluent la mise en place de systèmes de contrôle d'accès

stricts comprenant l'utilisation de la biométrie. En conséquence, de l'avis du CEPD, la mise en œuvre de systèmes de contrôle d'accès donnant lieu au traitement de données à caractère personnel, y compris des données biométriques, peut, en l'espèce, être raisonnablement considérée comme une mesure de contrôle interne nécessaire à la protection d'informations extrêmement sensibles et d'autres intérêts de l'Union.

III.3. Traitements portant sur des catégories particulières de données

Le traitement de données notifié ne concerne pas des données relevant des catégories de données visées à l'article 10, paragraphe 1, du règlement (CE) n° 45/2001.

III.4 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 doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et/ou traitées ultérieurement. Ce principe est appelé «principe de la qualité des données». En analysant la conformité avec ce principe du traitement en l'espèce, qui consiste essentiellement à traiter des données biométriques, le CEPD a noté ce qui suit.

(i) Responsabilité de l'évaluation générale de l'impact de la collecte des données: le CEPD comprend que le CCR-ITU a conclu que le traitement des données, y compris la collecte de données [biométriques] par rapport à d'autres données à caractère personnel, est nécessaire pour protéger les bâtiments du CCR-ITU. Toutefois, le CCR-ITU n'est pas parvenu à démontrer qu'il avait réalisé une analyse en profondeur de l'incidence de l'utilisation des données, examinant les raisons ayant justifié le recours à cette technologie et déterminant si d'autres solutions, portant moins atteinte à la vie privée, ont été envisagées. Dans une perspective d'avenir et plus particulièrement dans le cadre d'éventuelles actualisations du système, le CCR-ITU devrait procéder à une analyse d'impact appropriée qui, outre des aspects techniques et de sécurité, devrait également tenir compte de considérations liées à la protection des données et de la vie privée.

(ii) Évaluation de l'adéquation des personnes concernées dont les données sont traitées: ainsi qu'il est indiqué dans la notification, chaque membre du personnel du CCR-ITU est réputé être une personne concernée. En outre, la notification précise que le système en question est destiné à contrôler les identités et à autoriser ou refuser l'accès à toutes les entrées et sorties du CCR-ITU. En conséquence, chaque membre du personnel du CCR-ITU doit suivre les procédures d'enrôlement. Si l'ensemble du site (des bâtiments) du CCR-ITU est réputé constituer une installation nucléaire, il semble approprié pour CCR-ITU de ne pas limiter le nombre de personnes enrôlées à un groupe sélectionné ayant accès à certaines installations. Toutefois, les informations fournies au CEPD n'indiquent pas clairement si les membres du personnel travaillant à des fonctions (par exemple de nature administrative) exercées hors des zones nucléaires et des zones de sécurité devraient être soumis aux mêmes modalités de sécurité. À cet égard et par rapport aux possibles actualisations du système, le CEPD recommande au CCR-ITU d'étudier la possibilité de limiter l'enregistrement des codes [...] aux membres du personnel du CCR-ITU qui travaillent pour les zones nucléaires et les zones particulièrement sécurisées.

(iii) Évaluation de l'adéquation du type de données collectées: le type de données collectées, essentiellement des modèles [biométriques] et des données d'identification associées, correspond aux données que requiert l'exploitation d'un système de contrôle d'accès fondé

sur la biométrie. De ce point de vue, le CEPD estime que les données collectées sont adéquates et pertinentes au regard des finalités du traitement.

Loyauté et licéité. L'article 4, paragraphe 1, point a), du règlement exige que les données soient traitées loyalement et licitement. La question de la licéité a été analysée ci-dessus (voir point III.2.). Celle de la loyauté est étroitement liée à l'objet du point III.8, à savoir les informations fournies aux personnes concernées.

Exactitude. L'article 4, paragraphe 1, point d), du règlement dispose que les données à caractère personnel doivent être *«exactes et, si nécessaire, mises à jour»* et que *«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 sont principalement constituées de données biométriques, utilisées à des fins de contrôle d'accès. Certaines caractéristiques essentielles des systèmes biométriques ont une incidence directe sur le niveau d'exactitude des données générées pendant les phases soit d'enrôlement soit d'identification inhérentes à ce type de système. La question de l'exactitude des données se posera (ou non) selon si le système biométrique mis en place intègre ces caractéristiques essentielles. Nous décrivons ci-après ces caractéristiques essentielles et analysons la mesure dans laquelle elles ont été prises en compte dans le système biométrique examiné.

Premièrement, toute phase d'enrôlement doit prévoir des solutions de remplacement permettant d'identifier des personnes qui ne peuvent pas être enregistrées, ne serait-ce que temporairement. C'est ce qu'on appelle habituellement des «procédures de secours»[4]. En l'espèce, il est prévu qu'une vérification d'identification manuelle soit réalisée par les gardes du groupe de protection physique se tenant à l'entrée des zones de sécurité. Étant donné que les procédures de secours dans ce type de système sont très peu fréquentes (0 % après 12 sessions d'enrôlement), les procédures prévues par le CCR-ITU paraissent adéquates.

Deuxièmement, des mesures semblables doivent être prévues pour les personnes qui ont été correctement enregistrées, mais qui ne peuvent pas être identifiées (ce que l'on appelle généralement les «faux rejets»). Si ces mesures ne sont pas intégrées dans l'architecture du système, l'exactitude des informations générées par le système pourrait être compromise. En particulier, en cas de faux rejet, le système gardera trace du fait qu'une personne donnée, ne disposant pas des droits d'accès requis, a tenté d'accéder à une zone sécurisée, alors même que cette personne disposait des droits correspondants. Dans le même temps, puisque cette personne n'aura pas pu être identifiée, elle se verra refuser un droit (droit d'accès à des zones données) dont elle bénéficie.

En cas de faux rejet ou d'autres problèmes, la personne en question doit s'adresser au bureau des demandes du groupe de protection physique. Le CEPD estime que cette solution devrait limiter les tâches liées aux faux rejets.

Troisièmement, le système AECAPP du CCR-ITU se fonde sur des modèles [biométriques] stockés dans une base de données centrale associés à l'utilisation de lecteurs à caméra. Le CEPD note que cela donne lieu à l'utilisation de données biométriques aux fins de

[4] Pour une description des principes en matière de protection des données applicables dans le cadre des procédures de secours, voir l'avis du 13 octobre 2006 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).

l'identification et du contrôle d'accès en utilisant une comparaison avec un grand nombre (*«one-to-many»*). Ce type de mode de recherche ne mène pas toujours à des résultats corrects. En d'autres termes, il peut mal identifier des personnes et créer ainsi des enregistrements inexacts. Un autre mode de recherche tel que la comparaison de deux séries de données (*«one-to-one»*) ne présente pas le même problème car les données biométriques ne sont comparées qu'à un seul modèle plutôt qu'à un plus grand nombre de modèles. Le mode de recherche *«one-to-one»* implique généralement de stocker le modèle sur une puce détenue par la personne à identifier. Le modèle peut cependant aussi être stocké dans une base de données centrale, auquel cas il doit être accompagné d'un outil d'identification additionnel pouvant fonctionner comme suit. Par exemple une carte d'identification dotée d'une puce pourrait transmettre l'identité de la personne à l'unité d'identification, qui comparerait le modèle associé à l'identité de la personne aux données biométriques lui étant présentées à ce moment donné. En outre, comme décrit plus en détail ci-après, le mode de recherche *«one-to-one»* entraîne moins de traitement de données et contribue donc au respect du principe de proportionnalité.

En l'occurrence, l'AECAPP du CCR-ITU utilise un mode de recherche par comparaison avec un grand nombre (*«one-to-many»*). [...]. En principe, le CEPD estime plus adéquat d'utiliser le mode de recherche *«one-to-one»* où l'unité d'identification comparerait les [données biométriques] de la personne à un modèle unique (associé à l'identité). Comme souligné ci-dessus, un tel mode de recherche génère des résultats plus précis.

Le CEPD reconnaît qu'en l'espèce, compte tenu du nombre limité de modèles (environ 400), la possibilité d'erreurs est très réduite; toutefois, par principe, il est d'avis qu'il est plus approprié d'utiliser le mode *«one-to-one»*. Le mode de recherche *«one-to-one»* génère non seulement des informations plus précises, mais entraîne également moins de traitement de données dans la mesure où le système n'a qu'à vérifier la concordance de deux séries d'informations se rapportant à la même personne (contrairement à la vérification de la concordance d'une série d'informations par rapport aux modèles de nombreuses personnes). Ce mode de recherche porte donc intrinsèquement moins atteinte à la vie privée. En sélectionnant le mode de recherche *«one-to-one»*, les systèmes conservant des modèles biométriques sur des puces plutôt que dans des bases de données centrales sont plus respectueux de la vie privée. De toute évidence, le stockage sur des puces est plus respectueux de la vie privée car le modèle est conservé sur un support (p. ex. un badge à puce) qui reste en la possession de la personne concernée en question. Ainsi, la personne concernée a elle-même la maîtrise et la responsabilité directes de son modèle. Personne d'autre n'est en possession de son modèle ou n'y a accès. Un autre problème de la conservation dans des bases de données centrales est qu'elle entraîne le risque de recherches à l'aveuglette (*«fishing expeditions»*) utilisant la base de données pour des finalités autres que celles pour lesquelles elle a été conçue. Un système décentralisé résout ce risque sans dégrader le niveau de sécurité.

À la lumière de ce qui précède, le CEPD demande au CCR-ITU d'évaluer la décision qu'il a prise, et ce aux plans des choix technologiques discutés ci-dessus et du choix des meilleures techniques disponibles. Cette évaluation sera pertinente pour que le CEPD puisse apprécier la conformité de l'AECAPP avec l'article 4, paragraphe 1, point d), du règlement.

III.4. Conservation des données

L'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001 pose le principe que *«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». «L'institution ou l'organe communautaire prévoit, pour les données à caractère personnel qui doivent être conservées au-delà de la période précitée à des fins […] statistiques […], soit qu'elles ne seront conservées que sous une forme qui les rend anonymes, soit, si cela est impossible, qu'elles ne seront stockées qu'à condition que l'identité de la personne concernée soit cryptée».

D'après la notification, les données des visiteurs n'ayant pas accès à une zone nucléaire proprement dite sont conservées pendant 5 ans après leur dernière visite. La raison de la conservation de ces informations pendant cette durée est la suivante: les visiteurs sont pour la plupart des techniciens spécialisés ou des scientifiques de haut niveau qui visitent régulièrement le CCR- ITU, généralement pendant plusieurs années. Par conséquent, le CCR-ITU a décidé de conserver les données pendant 5 ans afin de pouvoir demander le renouvellement des habilitations de sécurité sans devoir collecter à chaque fois les données des personnes en question. Le CEPD comprend et admet la nécessité de conserver les données pour une telle durée au regard du type de données nécessaires pour le renouvellement d'une habilitation de sécurité.

Pour les visiteurs et le personnel de l'ITU ayant accès aux zones nucléaires proprement dites et dont les données de dosimétrie sont enregistrées, toutes les données seront conservées pendant 95 ans après la date de naissance de la personne concernée. Cela s'applique à toutes les données à l'exception des codes [...]. Elles sont conservées afin de pouvoir retrouver tout incident ou tout élément relatif aux valeurs de dosimétrie et pour pouvoir identifier et contacter la personne en question. Il s'agit d'une très longue durée. Toutefois, étant donné que le stockage de données précises de dosimétrie peut s'avérer significativement pertinent ultérieurement dans le contexte du traitement médical de la personne en question et/ou en vue d'éventuelles réclamations liées à des maladies professionnelles, le CEPD considère qu'il est possible d'estimer que cette durée se situe à l'intérieur d'une marge raisonnable.

D'après la notification, le CEPD comprend qu'aucune statistique sur les données à caractère personnel n'est autorisée après la période de conservation. Le CEPD souhaite toutefois souligner que lorsque de telles données sont utilisées au-delà de la période de conservation, elles doivent être rendues anonymes (article 4, paragraphe 1, point e), du règlement).

III.5 Transfert des données

D'après la notification, en cas d'incident de sécurité, les informations sont transférées à la DG ADMIN DS. Le CEPD rappelle que l'article 7 du règlement (CE) n° 45/2001 prévoit que les données à caractère personnel ne sont transférées *«que si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire»*. Pour respecter cette disposition, le responsable du traitement doit s'assurer, lorsqu'il communique des données à caractère personnel, que (i) le destinataire a les compétences requises et (ii) le transfert est nécessaire.

Les transferts susvisés, selon la notification, semblent relever de l'exécution légitime des missions entrant dans la compétence du destinataire concerné. En fait, «ADMIN DS» est compétente, entre autres, pour des missions liées à la protection du personnel, des bâtiments et des biens ainsi que celle des informations, de la transmission et du traitement des données. Pour assurer le plein respect de l'article 7 du règlement, le CEPD recommande qu'il soit rappelé à l'ensemble des destinataires qu'ils sont tenus de traiter ces données exclusivement aux fins pour lesquelles elles ont été transmises.

En cas d'incident de sécurité, ces informations peuvent être communiquées aux autorités compétentes nationales allemandes, auquel cas l'article 8 du règlement (CE) n° 45/2001 s'applique**.** L'article 8 du règlement (CE) n° 45/2001 prévoit plusieurs motifs juridiques autorisant le transfert d'informations à caractère personnel. Vu les circonstances de l'espèce, le responsable du traitement peut se prévaloir de l'article 8, point a), selon lequel les données à caractère personnel peuvent être transférées si elles doivent être utilisées pour exécuter une mission relevant de l'exercice de l'autorité publique ou si le transfert de données est réalisé dans l'intérêt légitime de la personne concernée. Vu qu'en vertu de l'article 8, point a), du règlement (CE) n° 45/2001 c'est au destinataire d'établir l'intérêt, le CEPD comprend que cette disposition signifie que si la transmission des informations n'est pas réalisée à la demande du destinataire, c'est au destinataire qu'il incombe d'en établir la nécessité.

Conformément à ce qui précède, lorsque les informations ne sont pas envoyées à la demande du destinataire, le responsable du traitement doit établir la nécessité du transfert des données. Afin de mettre cette règle en œuvre, le CEPD recommande que le responsable du traitement dresse la liste, dans un avis motivé, de tous les transferts de données qui seront ou ont été réalisés dans le contexte d'un cas donné et qu'il en décrive la nécessité. Ces procédures devraient être communiquées au personnel concerné.

III.6. Traitement des données pour le compte du responsable du traitement

En vertu de l'article 23 du règlement, si un traitement de données est réalisé par un sous-traitant pour le compte du responsable du traitement, un contrat ou un acte juridique doit être conclu entre le sous-traitant et le responsable du traitement. Le contrat doit prévoir que le sous-traitant agira selon les instructions du responsable du traitement (pour ce qui est du traitement des données). Le sous-traitant doit assurer la conformité avec les obligations de sécurité établies, en l'espèce, dans les règles nationales applicables mettant en œuvre l'article 17 de la directive 95/46.

En l'occurrence, le responsable du traitement utilise deux sous-traitants, l'un pour accomplir les tâches de protection physique (désigné «groupe de protection physique») et un autre pour entretenir et développer le logiciel et le matériel utilisés pour le traitement des données. Compte tenu du caractère extrêmement sensible des données, le CEPD tient à souligner qu'il est nécessaire que le responsable du traitement assure un très haut niveau de sécurité. Le CEPD comprend que le responsable des données a mis en place des accords et il n'a pas constaté de manquements à l'article 23 du règlement.

III.7. Droit d'accès et de rectification

Conformément à l'article 13 du règlement (CE) n° 45/2001, la personne concernée a le droit d'obtenir gratuitement du responsable du traitement, sans restriction, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information, 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 du règlement confère à la personne concernée le droit de rectifier les données inexactes ou incomplètes.

La notification décrit la manière dont un membre du personnel peut accéder aux données à caractère personnel le concernant et mentionne la possibilité qu'il a de les rectifier. La déclaration de confidentialité remise au CEPD pour examen indique l'adresse électronique à contacter pour l'exercice de ces droits. Le CEPD rappelle que ces droits s'appliquent non seulement aux informations fournies par la personne en question (données d'identification et modèles [biométriques]), mais également aux informations générées à chaque fois qu'une

personne accède au CCR-ITU. En conclusion, d'après les informations reçues, le CEPD n'a aucune raison d'estimer que les conditions des articles 13 et 14 du règlement ne seraient pas respectées.

III.8 Information de la personne concernée

Les articles 11 et 12 du règlement (CE) n° 45/2001 énumèrent les informations à fournir à la personne concernée. Ces articles présentent une liste d'informations obligatoires et une série d'autres informations. En l'espèce, toutes les données sont collectées directement auprès de la personne concernée, par conséquent il y a lieu d'observer les dispositions de l'article 11 (informations à fournir lorsque les données sont collectées auprès de la personne concernée).

Selon la notification, une déclaration de confidentialité sera disponible sur l'intranet du CCR-ITU et au poste de garde à l'entrée des locaux de l'ITU. La déclaration de confidentialité comprend les éléments suivants: (i) une explication du système d'autorisation d'entrée et de contrôle des accès de l'ITU; (ii) les informations à caractère personnel collectées, la fin à laquelle ces informations sont collectées et les moyens techniques utilisés pour cette collecte; (iii) les modalités de protection des informations; (iv) la durée de conservation des données; (v) la présentation des droits des personnes concernées (en termes d'accès, de modification et de suppression) et la mention du droit de saisir le CEPD. Le DPD a joint un projet de déclaration de confidentialité à la notification. Un exemplaire de la déclaration de confidentialité a été remis au CEPD.

Cette déclaration contient des informations sur les finalités du traitement et sur la manière dont le traitement est effectué, sur les conditions d'exercice du droit d'accès et de rectification, sur les délais de conservation des données et sur la possibilité de saisir le CEPD. Le CEPD estime que cette déclaration de confidentialité contient la plupart des informations requises en vertu des articles 11 et 12 du règlement. Néanmoins, il est d'avis que quelques modifications permettraient de garantir le plein respect de ces articles, en particulier:

- concernant la collecte des données biométriques, le personnel devrait recevoir des informations complémentaires, y compris sur le fonctionnement général du système et sur les conséquences concrètes d'un enregistrement ou d'un enregistrement impossible;
- davantage d'informations devraient être données sur les finalités du traitement, par exemple la politique de confidentialité ne mentionne pas la nécessité d'utiliser les informations pour une habilitation de sécurité auprès de la DG ADMIN DS.

Concernant la manière dont ces informations sont fournies, le CEPD est d'avis que la déclaration de confidentialité devrait être fournie aux personnes qui sont soumises à une procédure d'enrôlement. Il ne semble pas suffisant que cette déclaration soit disponible sur l'intranet ou à l'entrée des zones de sécurité. Dans une autre analyse de contrôle préalable[5], le CEPD a reconnu la procédure mise en place à la Banque centrale européenne (c'est-à-dire que la déclaration de confidentialité «sera fournie sur papier et les intéressés seront invités à la signer, précisant qu'ils l'ont lue et comprise»). Le CEPD estime qu'il s'agit là d'un moyen approprié de communiquer des informations et suggère que les intéressés reçoivent une copie de la déclaration de confidentialité, de manière à ce qu'ils puissent la consulter s'ils souhaitent, par exemple, savoir comment exercer leurs droits ou comment s'effectue le traitement des données.

[5] Voir l'avis sur le contrôle des accès de la Banque centrale européenne (2007-501).

III.9 Mesures de sécurité

Conformément à l'article 22 du règlement concernant la sécurité du traitement, «*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*». Après examen des mesures de sécurité décrites dans les informations fournies au CEPD, il n'y a pas de raison de penser que les mesures mises en œuvre dans le contexte de la procédure notifiée ne sont pas conformes à l'article 22 du règlement.

IV. Conclusion:

Rien ne permet de conclure à un manquement aux dispositions du règlement n° 45/2001, sous réserve que les considérations figurant dans le présent avis soient pleinement prises en compte. Le responsable du traitement doit en particulier:

- procéder à une évaluation de la décision de mettre en place le système de contrôle d'accès pour la protection physique tel que décrit au CEPD, en particulier évaluer la décision prise en termes de choix technologiques (utilisation de la [biométrie], utilisation du mode «*one-to-many*», nombre de personnes concernées touchées) et de choix des meilleures techniques disponibles. dans le contexte susvisé, reconsidérer s'il est adéquat d'appliquer les mesures à tous les membres du personnel du CCR-ITU;
- dans le contexte de l'évaluation susvisée, évaluer la mise en œuvre possible au regard des futures modifications du système en termes de choix technologiques;
- présenter l'évaluation susvisée (un rapport) au CEPD dans un délai de 8 à 10 mois;
- informer les destinataires des données que les données à caractère personnel peuvent uniquement être traitées aux fins qui ont motivé leur transmission et dresser la liste, dans un avis motivé, de tous les transferts de données réalisés vers les autorités et en décrire la nécessité. Ces procédures devraient être communiquées au personnel concerné;
- modifier la déclaration de confidentialité conformément aux recommandations du présent avis et s'assurer qu'une copie de cette déclaration est remise aux personnes concernées ou qu'elle est mise à leur disposition afin qu'elles puissent la consulter.

Fait à Bruxelles, le 24 juillet 2012

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données