Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission sur le contrôle de fiabilité de sécurité au Centre commun de recherche d'Ispra

Bruxelles, le 19 juin 2013 (Dossier 2012-1090)

1. Procédure

Le 20 décembre 2012, le délégué à la protection des données (DPD) de la Commission a soumis au contrôleur européen de la protection des données (CEPD) une notification en vue d'un contrôle préalable concernant les traitements réalisés dans le cadre du contrôle de fiabilité de sécurité au Centre commun de recherche d'Ispra (ci-après le «CCR Ispra»).

Cette notification fait suite à la décision du directeur général du CCR du 11 juillet 2012 de supprimer la procédure de contrôle «nulla osta» mise en place pour le recrutement des candidats retenus sur les sites du CCR. Cette décision résulte d'une inspection menée au CCR en 2010 (dossier 2010-0832), à l'issue de laquelle le CEPD a mis en cause la licéité de la procédure «nulla osta» en vigueur au CCR.

En lieu et place de cette procédure, le CCR présente une proposition de procédure de contrôle de fiabilité de sécurité intulée «Contrôle de fiabilité» de sécurité. Cette procédure n'est plus associée au recrutement du personnel de tous les sites du CCR[1] à l'exception de Karlsruhe, mais à l'accès non accompagné aux zones nucléaires et aux zones sensibles connexes du site d'Ispra. La portée a donc été sensiblement réduite à la fois en termes du nombre de personnes concernées et des zones physiques concernées.

Dix annexes ont été jointes à la notification. L'une d'elles, une note au dossier, fournit des informations sur la mise en œuvre de certaines des recommandations spécifiques contenues dans le rapport d'inspection qui a abouti à l'élaboration du contrôle de fiabilité de sécurité.

Comme l'explique la note au dossier, afin de préserver la nécessité de maintenir des mesures de sécurité spécifiques pour les zones à risque élevé, les directeurs peuvent mettre en œuvre les contrôles de sécurité nécessaires. Cette possibilité est toutefois très limitée par nature, étant donné
- qu'elle ne peut être imposée qu'à l'accès aux zones réglementées, avec l'indication «nucléaire» (contrairement à la procédure «nulla osta» qui a été supprimée et qui s'appliquait au recrutement du personnel),

[1] Le CCR a supprimé la procédure «nulla osta» pour ses sites de Petten, Séville, Geel et Bruxelles et cette procédure a également été supprimée pour le site d'Ispra, quoiqu'en maintenant un contrôle de sécurité pour l'accès aux «zones sensibles» (y compris les zones nucléaires).

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
E-mail: edps@edps.europa.eu – Site internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

- lorsqu'elle est requise par les normes de la Commission et/ou les règles locales, régionales et/ou nationales applicables en matière de sécurité et
- conformément aux règles relatives à la protection des données.

Dans les échanges avec le CCR, il a été précisé que le CCR dispose d'un mandat spécifique découlant d'un protocole d'accord («protocole») conclu entre la direction de la sécurité de la direction générale chargée des ressources humaines et de la sécurité («DG.HR.DS») et le Centre commun de recherche pour mener certains types d'enquêtes de sécurité.

À l'issue d'une première analyse de la notification, le 9 janvier 2013, le CEPD a pris contact à la fois avec le DPD et le CCR, en tant que responsable du traitement, en soulignant que la notification n'était pas conforme au troisième rapport de suivi adressé par le CEPD au CCR. Dans cette lettre, le CEPD a insisté sur la nécessité de fonder la procédure sur la nouvelle décision relative à la sécurité et sur le protocole d'accord. En effet, comme indiqué dans le courriel, au moment de l'analyse, la décision C(94)2129 de la Commission relative à la sécurité, qui définit les tâches générales du service de sécurité, était en cours de révision. Comme expliqué dans la note au dossier, le projet de nouvelle décision inclut un article sur «*la mesure de sécurité que la Commission peut prendre, sous réserve du respect strict des droits fondamentaux et des principes de légalité, de transparence, de responsabilité, de subsidiarité et de proportionnalité. La description de ces mesures couvre, notamment, des contrôles de sécurité a priori des personnes accédant aux sites afin de prévenir et de contrôler les menaces à la sécurité*». Le projet contient également une disposition prévoyant la possibilité que certains contrôles de sécurité soient – par la signature d'un acte d'exécution – réalisés au niveau local, comme le service de sécurité du CCR Ispra. Cela conduira à l'adoption d'un nouveau protocole d'accord.

Au moment de la rédaction du présent avis, les discussions entre la DG.HR.DS et le CCR étaient toujours en cours.

Dans le même temps, le CCR se trouve dans une situation dans laquelle il doit appliquer des contrôles de sécurité obligatoires pour l'accès à ses zones réglementées nucléaires. Le CCR doit se conformer à la recommandation 4.26 du document (INFCIRC/225/fifth) de l'Agence internationale de l'énergie atomique, qui prévoit que «les personnes habilitées à accéder non accompagnées à la zone protégée devraient être limitées à celles dont la fiabilité a été contrôlée», et au plan de protection physique approuvé dans un décret du ministère italien de l'industrie.

Par conséquent, le CEPD a décidé de mener son analyse juridique sur la base des informations reçues, même si la nouvelle décision de la Commission et le protocole d'accord ne sont pas finalisés, afin d'éviter une lacune sur le plan de la sécurité. Le CEPD a eu accès, par le biais de la note du CCR, aux parties pertinentes du projet de décision et a été informé par le CCR que le nouveau protocole d'accord ne différerait que légèrement du protocole actuel.

Le présent avis est donc formulé sans préjudice de tout commentaire additionnel que le CEPD pourrait formuler lorsque la nouvelle décision relative à la sécurité et le nouveau protocole d'accord seront adoptés.

Le 31 mai 2013, le projet d'avis du CEPD a été envoyé au DPD pour commentaires. Ces derniers ont été reçus le 14 juin 2013.

2. Examen de la question

2.1 Les faits

La ***finalité*** du traitement des données à caractère personnel est de déterminer et de confirmer la fiabilité des personnes ayant besoin de bénéficier d'un accès non accompagné aux zones nucléaires et aux zones sensibles connexes du CCR Ispra.

Les pièces justificatives nécessaires au traitement des «contrôles de fiabilité» de sécurité incluent un curriculum vitae récent ou un formulaire de candidature, à l'exception du personnel externe ayant conclu un contrat de fourniture ou de service avec la Commission européenne, pour lequel un extrait de casier judiciaire est également requis. Un «Permesso di soggiorno» est également nécessaire pour les résidents non italiens.

À l'issue du nouveau «contrôle de fiabilité» de sécurité, les unités «Ressources humaines» et «Recrutement» appliquent actuellement l'article 28, point c), du Statut des fonctionnaires des Communautés européennes concernant le recrutement, en insistant sur les garanties de moralité requises pour l'exercice de fonctions spécifiques. Des articles identiques sont appliqués par analogie aux autres types d'agents temporaires.

La notification souligne que les informations concernant la présence sur le site de personnes pour permettre d'appliquer la décision C(2004)1597 de la Commission relative à la durée maximale du recours au personnel non permanent dans les services de la Commission ne sont plus traitées ni collectées par le service de sécurité.

S'agissant des ***personnes concernées***, le traitement s'applique à tout membre du personnel ayant besoin d'un accès non accompagné aux zones nucléaires et aux zones ou informations sensibles connexes sur le site d'Ispra (c'est-à-dire devant subir un «contrôle de fiabilité» de sécurité). Il est à noter que cela ne concerne pas les visiteurs quotidiens qui pénètrent occasionnellement sur le site et devront être accompagnés à tout moment s'ils visitent des zones sensibles du CCR Ispra et ces données ne seront conservées que dans le SECPAC (2007-0381).

Les ***données traitées*** sont classées dans les catégories suivantes : personnes, documents et types de document.

- PERSONNES: prénom, prénom réel, nom, nom réel, nom de présentation, sexe, titre, date de naissance, lieu de naissance, pays de naissance, nationalité, pseudonyme, numéro de personnel, identificateur de la source, source, adresse électronique, numéro de téléphone, date de début et date de fin, [identificateur universel].

- TYPES DE DOCUMENT: formulaire de candidature ou, à titre subsidiaire, curriculum vitae, extrait récent de casier judiciaire (uniquement pour le personnel externe, ayant conclu un contrat de fourniture ou de service avec la Commission européenne), copie du contrat de fourniture ou de service concerné (numéro de référence) (pour le personnel externe), Permesso di Soggiorno (pour les résidents non italiens), autocertification, habilitation, formulaire de collecte de données et dérogation.

Conformément à la notification, les champs de données sont associés aux pièces justificatives présentées et, pour l'essentiel, ne relèvent pas du champ d'application de l'article 10 du règlement. Il est également indiqué que certains documents peuvent finalement relever de l'article 10.

Quant au caractère obligatoire de ces informations, la notification prévoit que, lors du recrutement, les membres du personnel soient informés par les responsables des ressources humaines du fait qu'ils doivent fournir certaines pièces justificatives et que les données les concernant peuvent être utilisées aux fins de l'application du Statut et par le service de sécurité pour réaliser un «contrôle de fiabilité» de sécurité si leur emploi implique l'accès à des zones nucléaires ou à des zones ou informations sensibles connexes.

Cette question particulière, tout comme quelques autres, est détaillée et régulièrement expliquée dans les «Newcomer's Security Briefings» (contrôle de sécurité des nouveaux venus) bimensuels.

La ***responsabilité première du traitement des données*** incombe à l'unité chargée de la sûreté et de la sécurité du CCR Ispra. Elle fait rapport directement au directeur du site d'Ispra.

Quant à la ***durée de conservation*** des données, la notification prévoit que les données doivent être conservées aussi longtemps qu'il existe un lien contractuel avec la personne concernée et qu'elles doivent, néanmoins, être conservées pendant deux années supplémentaires après la conclusion dudit lien contractuel, à savoir la retraite, la limite de la durée du contrat temporaire, etc.

Par conséquent, toutes les données documentaires et à caractère personnel relatives aux contrôles de fiabilité seront supprimées ou rendues anonymes à l'expiration de ce délai. À titre exceptionnel, ces informations pourraient être conservées plus longtemps, si cela est dûment justifié pour permettre d'enquêter sur des violations de la sécurité ou des incidents relatifs à la personne concernée après son départ du site d'Ispra.

En ce qui concerne les données collectées pour les candidats qui renoncent à leur candidature ou ne sont pas recrutés mais ont subi un contrôle de sécurité de fiabilité, les données sont conservées pendant un an.

Les données à caractère personnel collectées et toutes les informations relatives au traitement susvisé sont stockées sur des serveurs dédiés du service de sécurité du CCR Ispra, dont l'exploitation est subordonnée aux décisions et dispositions de la Commission en matière de sécurité des TI pour ce type de serveurs et de services.

L'accès aux données se fait par un accès individuel unique protégé par un identifiant/mot de passe. Au sein du personnel de base du service de sécurité, on trouve également plusieurs profils, comme le *responsable sécurité*, *l'archiviste sécurité et l'administrateur*. Les *responsables sécurité* peuvent avoir accès à des données à caractère personnel. Les *archivistes sécurité* peuvent avoir accès à toutes les informations enregistrées, y compris les données documentaires. Les *administrateurs* ont plein accès à l'ensemble des fonctions ARDOS, y compris à la gestion de ces profils.

À l'heure actuelle, une série de procédures semi-automatisées est utilisée pour procéder à cette analyse de la durée de conservation, en raison des multiples et divers scénarios possibles, mais une intervention manuelle est nécessaire pour supprimer des données documentaires d'ARDOS, qui sont exclusivement conservées sous forme numérique.

La notification indique également que le service de sécurité a supprimé et contrôlé tous les documents papier qu'il a conservés plus longtemps que le délai susmentionné et qui ne sont

plus nécessaires. Le CCR a précisé qu'en ce qui concerne les documents historiques collectés dans le cadre de la procédure «nulla osta», le CCR a effectivement détruit tous les documents stockés en format papier qui étaient en sa possession. S'agissant d'autres documents électroniques éventuels collectés aux fins du contrôle «nulla osta», le CCR affirme qu'une procédure qui permettra de supprimer toutes les informations pouvant être identifiées comme exclusivement liées à la procédure «nulla osta» (comme les formulaires de candidature, les CV, etc.) est en voie d'élaboration et sera mise en place à la fin 2013.

S'agissant des ***destinataires*** des données, les pièces justificatives nécessaires au traitement des «contrôles de fiabilité» de sécurité conservés dans ARDOS sont destinées à l'usage interne du service de sécurité. Les données proprement dites ne sont jamais transférées ou accessibles directement de l'extérieur du service de sécurité, étant donné que ce système d'information est situé dans un réseau physiquement isolé.

Les «contrôles de fiabilité» de sécurité constituant un processus interne au service de sécurité, ils n'impliquent aucun type de fourniture d'information à d'autres personnes. Seul le personnel de base du service de sécurité ayant subi un contrôle de sécurité peut accéder à ces données. Le directeur du site d'Ispra peut demander des informations supplémentaires en cas d'urgence ou d'enquête de sécurité.

S'agissant du ***droit à l'information***, une déclaration spécifique de confidentialité était jointe à la notification et souligne que les personnes privées peuvent poser des questions concernant ce traitement. Elle indique que les demandes peuvent être adressées au responsable du traitement par l'intermédiaire d'une boîte de messagerie électronique fonctionnelle servant de point de contact unique et elle en fournit les coordonnées. La déclaration précise que la finalité du traitement de données à caractère personnel est de déterminer et de confirmer la fiabilité des personnes associées à une demande d'habilitation à long terme.

Quant à la déclaration de confidentialité proprement dite, elle contient des informations sur la finalité du traitement (avec une brève description), l'identité du responsable du traitement, la base juridique applicable, les destinataires des données, la conservation des données ainsi que la durée de conservation de celles-ci. Elle contient également des informations sur les droits d'accès et de rectification. Enfin, elle évoque également le droit de recours devant le contrôleur européen de la protection des données.

Pour ce qui est des ***droits d'accès et de rectification***, dans un souci de transparence, le service de sécurité du CCR Ispra a envisagé une procédure par laquelle les personnes concernées peuvent demander et vérifier quelles sont les données enregistrées les concernant. Le point de contact unique du service de sécurité du CCR Ispra est responsable de la fourniture d'accès aux données à caractère personnel ou de leur correction. Une procédure spécifique pour la mise à jour ou le renvoi d'un «extrait de casier judiciaire original» a été mise en place. Cette demande doit être faite en utilisant le «formulaire de renvoi ou d'actualisation de l'extrait original de casier judiciaire». Ceci ne concerne actuellement que le personnel externe.

Sur demande justifiée de la personne concernée, les données seront modifiées, gelées ou éventuellement effacées dans un délai maximal de 14 jours.

S'agissant des ***mesures de sécurité***, la notification renvoie aux réponses détaillées faites aux questions relatives à la mise en œuvre des mesures techniques et organisationnelles adoptées pour ARDOS.

[...]

2.2. Aspects juridiques

2.2.1. Contrôle préalable

Le présent avis de contrôle préalable concerne le traitement de données à caractère personnel dans le cadre des contrôles de fiabilité de sécurité du CCR Ispra. Le traitement est réalisé par une institution européenne, dans l'exercice d'activités qui relèvent du champ d'application du droit de l'UE (article 3, paragraphe 1, du règlement). Le traitement de données à caractère personnel est effectué, à toute le moins en partie, de façon automatisée (article 3, paragraphe 2, du règlement). En conséquence, le règlement s'applique.

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*». L'article 27, paragraphe 2, du règlement dresse une liste des traitements susceptibles de présenter de tels risques.

Selon le CCR, en tant que responsable du traitement, le traitement des données relève de l'article 27 pour ce qui concerne :
(a) les condamnations pénales ou les mesures de sûreté ;
(b) les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, essentiellement leur comportement ;
(c) les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.

En premier lieu, ces traitements de données relèvent de l'article 27, paragraphe 2, point a), du règlement (CE) n° 45/2001, qui dispose que les traitements de données relatives à «*des suspicions, infractions, condamnations pénales ou mesures de sûreté*» sont soumis au contrôle préalable du CEPD. Dans le cas d'espèce, en traitant les données susvisées, le service de sécurité peut traiter des informations pouvant se rapporter à des suspicions ou à des condamnations pénales. La référence à la notion de mesures de sûreté à l'article 27, paragraphe 2, point a), n'est pas pertinente étant donné que la notion de mesures de sûreté n'est pas interprétée comme couvrant les mesures décrites[2].

En outre, la notification relève également de l'article 27, paragraphe 2, point b), du règlement (CE) n° 45/2001, qui dispose que les traitements destinés à «*évaluer des aspects de la personnalité des personnes concernées, tels que leur (...) comportement*» sont soumis au contrôle préalable du CEPD. Dans le cas d'espèce, le comportement de personnes physiques sera évalué afin de déterminer leur fiabilité, ce qui déclenche l'application de l'article 27, paragraphe 2, point b).

Enfin, le CEPD ne considère pas que l'article 27, paragraphe 2, point d), soit applicable en l'espèce. En effet, cette disposition concerne les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat (ceci concerne généralement des listes noires). Tel ne semble pas être la finalité du contrôle de fiabilité, dont le but est, au contraire, de permettre un accès non accompagné au site du CCR.

Contrôle préalable ex ante. Le contrôle préalable étant conçu pour répondre à des situations susceptibles de présenter certains risques, l'avis du CEPD devrait être rendu avant le début du

[2] En effet, l'article 27, paragraphe 2, point a), fait référence à ce que l'on appelle des «mesures de sûreté», comme indiqué dans la version française du règlement.

traitement. En l'espèce, le traitement devrait remplacer la procédure «nulla osta» et, partant, être examiné ex ante et toute recommandation devrait être prise en compte avant la mise en œuvre de la procédure.

Notification et délai de présentation de l'avis du CEPD. La notification du DPD a été reçue le 20 décembre 2012. L'analyse a été suspendue entre le 9 janvier 2013 et le 23 avril 2013, date à laquelle la suspension a été levée. Le projet a été envoyé pour commentaires le 31 mai 2013 et ceux-ci ont été reçus le 14 juin 2013. Par conséquent, la période de deux mois dont dispose le CEPD pour rendre un avis a été suspendue pendant 104 jours + 14 jours pour permettre au DPD et au CCR en tant que responsable du traitement de commenter le projet d'avis du CEPD. L'avis devait donc être adopté au plus tard le 19 juin 2013.

2.2.2. Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que pour les motifs visés à l'article 5 du règlement (CE) n° 45/2011.

La notification mentionne que la licéité du traitement relève de l'article 5, points a), b), d) et e), du règlement. Cependant, parmi les différents motifs énoncés à l'article 5 du règlement (CE) n° 45/2001, le CEPD estime que le traitement notifié en vue d'un contrôle préalable ne relève que de l'article 5, point b), en vertu duquel «*le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis*» et de l'article 5, point a), en vertu duquel le traitement de données ne peut être effectué que si le traitement 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* (...)».

Comme indiqué dans la section relative à la procédure, le CCR doit se conformer à la recommandation 4.26 du document (INFCIRC/225/fifth) de l'Agence internationale de l'énergie atomique, qui prévoit que «les personnes habilitées à accéder non accompagnées à la zone protégée devraient être limitées à celles dont la fiabilité a été contrôlée», et au plan de protection physique approuvé dans un décret du ministère italien de l'industrie et que, de ce fait, l'article 5, point b), du règlement s'applique. Le CCR Ispra en tant qu'opérateur nucléaire et titulaire d'une licence nucléaire conforme au droit italien est dans l'obligation de mettre en œuvre de nombreuses mesures de sécurité différentes.

Comme indiqué dans son troisième rapport de suivi d'inspection du 5 décembre 2012, le CEPD a recommandé que cette obligation légale soit complétée par la nouvelle décision de la Commission relative à la sécurité et par le protocole d'accord mis à jour. En effet, le décret italien et l'AIEA énoncent le principe du contrôle de fiabilité, mais ne précisent ni comment ni par qui il doit être réalisé (service de sécurité du CCR ou DG.HR.DS). De plus, si l'on peut déduire de la recommandation de l'AIEA que le contrôle de la fiabilité impliquera la collecte et le traitement de données à caractère personnel, la recommandation proprement dite n'impose pas le traitement de données à caractère personnel.

C'est pourquoi la future nouvelle décision de la Commission relative à la sécurité et le protocole d'accord mis à jour entre la DG CCR et la DG HR jouent un rôle crucial dans le renforcement de la capacité du CCR à réaliser des contrôles de sécurité et, partant, dans le renforcement de la licéité et de la légitimité du traitement dans le cadre du contrôle de fiabilité de sécurité.

Tant la nouvelle décision de la Commission relative à la sécurité que le nouveau protocole d'accord devront être transmis au CEPD pour analyse, dans la mesure où ils complètent les motifs juridiques actuels fondés sur l'article 5, point b) (loi italienne), et sur l'article 5, point a).

De ce fait, le CEPD prend note des actes législatifs suivants, qui établissent les motifs juridiques justifiant les traitements réalisés dans le cadre d'enquêtes :

- loi italienne n° 906/1960 concernant la création du Centre commun de recherche d'Ispra ;

- plan de protection physique approuvé par décret du ministère italien de l'industrie, qui inclut toutes les mesures supplémentaires complétant celles citées dans le document INFCIRC/225 de l'AIEA[3], et implicitement considéré comme la base de ce document ;

- décision de la Commission du 8 septembre 1994 relative aux tâches du bureau de sécurité de la Commission européenne[4], **révisée une fois;**

- protocole d'accord conclu entre la direction générale «Ressources humaines et sécurité» » et le «Centre commun de recherche» concernant les tâches réalisées dans le domaine de la sécurité (une version actualisée suivra l'adoption de la nouvelle décision de la Commission relative à la sécurité), **mise à jour une fois.**

Quant à la nécessité du traitement, outre la référence à la nouvelle décision de la Commission relative à la sécurité et au nouveau protocole d'accord, le CEPD considère que le traitement est nécessaire pour se conformer au droit international et italien relatif aux installations nucléaires.

Compte tenu de la décision prochaine et du nouveau protocole, le CEPD considère que la base juridique prévoit les tâches des services de sécurité du CCR Ispra, sur la base des règles existantes applicables à la Commission européenne.

2.2.3. Traitement portant sur des catégories particulières de données

Compte tenu du fait que la finalité du traitement est de déterminer et de confirmer la fiabilité des personnes ayant besoin d'un accès non accompagné aux zones nucléaires et aux zones sensibles connexes du CCR Ispra, certains documents pourraient éventuellement relever de l'article 10.

À cet égard, le CEPD rappelle l'article 10, paragraphe 5, du règlement (CE) n° 45/2001, qui dispose que «*[l]e traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que s'il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, par le contrôleur européen de la protection des données*». En l'espèce, une dérogation est prévue par l'article 10, paragraphe 5, en vertu duquel ce traitement est autorisé en raison des obligations légales associées à la mise en œuvre du «Plan de protection physique» que le Centre commun de recherche est tenu de mettre en œuvre (voir les instruments juridiques mentionnés au point 2.2.2 ci-dessus).

[3] http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf

[4] La décision C(2001)3031 de la Commission (aussi 2001/844/CE) et la décision C(2007)513/Euratom de la Commission mentionnées dans la notification ne sont pas considérées comme les principaux documents pertinents en l'espèce.

2.2.4. Qualité des données

Conformément à 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 ou pour lesquelles elles sont traitées ultérieurement*».

Les données traitées dans le cadre du contrôle de fiabilité de sécurité semblent limitées à ce qui est nécessaire pour répondre à la finalité du traitement et, partant, elles sont conformes à l'article 4, paragraphe 1, point c), du règlement (CE) n° 45/2001.

S'agissant de l'extrait de casier judiciaire, le CCR utilise l'expression «police record» en anglais. Comme indiqué dans la procédure concernant l'inspection au CCR (2010-0834), le CEPD a déjà indiqué que cette expression ne devait pas être utilisée. Seul un extrait de casier judiciaire délivré par l'autorité compétente du pays concerné peut être collecté. Par conséquent, des documents comme un «certificat de bonne vie et mœurs» ou tout autre document analogue ne devraient pas être collectés, sauf lorsqu'il n'existe pas de casier judiciaire national dans le pays concerné. Par ailleurs, le CEPD rappelle que le CCR a créé une liste des «extraits de casier judiciaire» pour tous les États membres dans les langues d'origine. Ce document est celui qui devrait être demandé. Le CEPD invite donc le CCR à modifier l'expression actuellement utilisée dans la procédure prévue. En outre, étant donné le nombre de ressortissants étrangers concernés, les candidats devraient également être informés du fait que l'extrait de casier judiciaire doit être délivré par leur pays de résidence actuelle et/ou passée et/ou par leur pays d'origine.

Conformément à l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel doivent être «*exactes et, si nécessaire, mises à jour*» et «*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*».

S'agissant de l'extrait de casier judiciaire, la période pendant laquelle ce document peut être considéré comme exact est très limitée. Le CEPD invite donc le CCR à évaluer la nécessité de conserver un tel extrait pendant une longue période (voir également le point 2.2.5 ci-dessous).

2.2.5. Conservation/rétention 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*».

Le traitement prévoit des délais de conservation différents.

1) Le CCR prévoit de conserver les données aussi longtemps qu'il existe un lien contractuel avec la personne concernée (qu'il s'agisse de personnel interne ou externe). Un délai supplémentaire de deux ans après la conclusion du lien contractuel est également prévu (retraite, limites de la durée du contrat temporaire, etc.).

Le CEPD prend note que le CCR considère que ce délai de conservation est nécessaire au traitement relatif à la fiabilité. Toutefois, en ce qui concerne l'extrait de casier judiciaire et

compte tenu de l'analyse ci-dessus, les données contenues dans un tel extrait ne peuvent être considérées comme exactes que pendant une période limitée. Le CEPD met donc en doute la durée de conservation de l'extrait de casier judiciaire, qui devrait, selon lui, être limitée à un maximum de deux ans après sa présentation. En effet, cela coïnciderait avec le délai durant lequel la Cour des comptes vérifierait ce document (pour traitement ultérieur). Les extraits qui ont été contrôlés par la Cour des comptes avant l'expiration de ce délai pourraient être détruits plus tôt. Cette interprétation a été formellement acceptée par la Cour des comptes. Le délai de conservation prévu dans la notification et la déclaration de confidentialité devrait être modifié en ce sens.

2) Après le délai mentionné au point 1, il est prévu que toutes les données documentaires et à caractère personnel relatives aux *contrôles de fiabilité* soient supprimées ou rendues anonymes mais que, à titre exceptionnel, elles puissent être conservées plus longtemps si cela est dûment justifié pour permettre d'enquêter sur les violations ou les incidents de sécurité se rapportant à la personne concernée après son départ du site d'Ispra.

Le CEPD prend note du fait que le CCR Ispra considère que ce délai de rétention est nécessaire aux fins d'un traitement ultérieur en cas d'enquêtes. Le CEPD tient à insister sur le fait qu'une telle rétention devrait néanmoins être exceptionnelle et dûment justifiée.

En ce qui concerne les données collectées pour les candidats qui renoncent à leur candidature ou qui ne sont pas recrutés mais ont subi un *contrôle de fiabilité de sécurité,* les données sont conservées pendant un an. Le CEPD prend note de ce délai de conservation.

Le CCR mentionne également dans la notification que le service de sécurité a supprimé et contrôlé tous les documents papier qui ont été conservés plus longtemps que le délai susvisé et qui ne sont plus nécessaires. Le CEPD comprend que cela concerne les documents relatifs à la procédure «nulla osta» qui ont été collectés au fil des années avant que le directeur général du CCR ne décide de supprimer cette procédure. En effet, bien que le CEPD se félicite qu'une procédure soit prévue pour toute nouvelle donnée traitée dans le cadre du contrôle de fiabilité de sécurité, il est également important que le CCR établisse des règles sur les données existantes.

2.2.6. Transfert de données

Compte tenu des informations fournies, seul l'article 7 du règlement (CE) n° 45/2001 s'applique. En effet, les données proprement dites ne sont jamais directement transférées ou accessibles depuis l'extérieur du service de sécurité, étant donné que le système d'information est situé dans un réseau physiquement isolé. Par ailleurs, seul le personnel de base du service de sécurité ayant subi un contrôle de sécurité peut accéder aux données. Le directeur du site d'Ispra peut demander des informations supplémentaires en cas d'urgence ou d'enquête de sécurité. Comme indiqué dans les documents reçus (déclaration de confidentialité), le service de sécurité, qui est chargé de la gestion de l'accès au site d'Ispra, peut également transférer les données à la direction «Sécurité» (DG.HR.DS) de la Commission pour des raisons de sécurité.

Des données peuvent faire l'objet de transferts vers des institutions et organes de l'Union européenne comme l'OLAF, l'IDOC, le CEPD ou le Médiateur européen, dans leur domaine de compétence.

Étant donné les compétences des organes destinataires, il apparaît que ces transferts de données sont nécessaires à l'exécution légitime de missions relevant de la compétence des destinataires. En outre, les nouvelles règles de sécurité devront également distinguer clairement entre les

compétences du CCR et celle réservées à la DG.HR.DS en ce qui concerne la sécurité et les cas dans lesquels ces transferts peuvent avoir lieu.

En tout état de cause, le destinataire doit être informé que, en vertu de l'article 7, paragraphe 3, les données ne peuvent être traitées qu'aux fins qui ont motivé leur transmission.

Aucun transfert de données à caractère personnel n'est prévu vers des États membres ou des pays tiers.

2.2.7. Droits d'accès et de rectification

Le droit d'accès est le droit de la personne concernée d'être informée de toute information la concernant qui fait l'objet d'un traitement par le responsable du traitement. Aux termes de l'article 13 du règlement (CE) n° 45/2001, la personne concernée a le droit d'obtenir, sans contrainte, 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.

La déclaration de confidentialité mentionne que les personnes physiques adressent leurs questions (afin de vérifier quelles données à caractère personnel sont conservées, de les faire rectifier, corriger ou supprimer) concernant ce traitement au responsable du traitement. Elle mentionne une boîte de messagerie électronique fonctionnelle comme personne de contact pour exercer ce droit.

2.2.8. Information de la personne concernée

Conformément aux articles 11 et 12 du règlement (CE) n° 45/2001, le responsable du traitement est tenu d'informer les personnes auxquelles les données se rapportent que des données les concernant sont collectées et traitées. L'article 11 traite des informations à fournir lorsque les données sont collectées auprès de la personne concernée, tandis que l'article 12 concerne les informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée. Les personnes ont également le droit d'être informées, entre autres choses, des finalités du traitement, des destinataires des données et des droits spécifiques dont disposent les personnes physiques en tant que personnes concernées.

En tant que responsable du traitement, le CCR a fourni une déclaration de confidentialité couvrant le contrôle de fiabilité de sécurité. La notification ne contient toutefois aucune information sur la manière dont cette déclaration de confidentialité est communiquée aux personnes concernées. La notification contient la déclaration suivante : «Lors du recrutement, le personnel est informé par les responsables des ressources humaines qu'ils doivent fournir certains documents et que leurs données peuvent être utilisées aux fins de l'application du Statut et par le service de sécurité en vue de l'exécution d'un «contrôle de fiabilité» de sécurité si leur poste implique l'accès à des zones nucléaires ou à des zones ou informations sensibles connexes. Par conséquent, le CEPD tient à souligner que la déclaration de confidentialité devrait être fournie à ce moment. Ceci devrait être clairement indiqué dans la procédure. Par ailleurs, en ce qui concerne le personnel externe d'un sous-traitant, la déclaration de confidentialité devrait être fournie au moment de la collecte des données.

Le CEPD a également examiné le contenu des informations visées dans la déclaration de confidentialité et considère qu'elle contient les informations requises au titre des articles 11 et 12 du règlement (CE) n° 45/2011. En effet, elle contient des informations sur la finalité du

traitement (avec une brève description), l'identité du responsable du traitement, la base juridique pertinente, les destinataires des données, la conservation des données ainsi que les délais de conservation des données et une boîte de messagerie électronique fonctionnelle pour les questions. Cependant, il conviendra de faire référence à la nouvelle décision de la Commission relative à la sécurité et au nouveau protocole d'accord, dès qu'ils auront été adoptés.

2.2.9. Mesures de sécurité

Conformément aux articles 22 et 23 du règlement (CE) n° 45/2001, le responsable du traitement doit mettre 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 de sécurité doivent, notamment, 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.

[...]

Le CEPD n'a donc pas de raison de croire que le CCR n'a pas mis 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.

3. Conclusion

Rien ne permet de conclure à une violation des dispositions du règlement (CE) n° 45/2001, pour autant que les considérations énoncées dans le présent avis soient pleinement prises en compte. Le CCR Ispra doit, en particulier, mettre en œuvre les dispositions suivantes:

- se conformer aux délais de conservation des données prévues pour le traitement de l'extrait de casier judiciaire ;
- prévoir que la déclaration de confidentialité soit remise aux différentes personnes concernées (personnel interne et externe) aux moments adéquats et qu'elle soit modifiée en conséquence, comme indiqué plus haut ;
- fournir au CEPD les documents pertinents constituant la base juridique (nouvelle décision de la Commission européenne relative à la sécurité et nouveau protocole d'accord) dès qu'ils seront disponibles.

Fait à Bruxelles, le 19 juin 2013

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données