Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne concernant les avis de sécurité sur les ressortissants de pays tiers accédant aux sites du Centre commun de recherche

Bruxelles, le 22 juillet 2014 (Dossier 2013-1020)

1. Procédure

Le 17 septembre 2013, le délégué à la protection des données (ci-après, le «DPD») de la Commission européenne (ci-après, la «Commission») a soumis au contrôleur européen de la protection des données (ci-après, le «CEPD») une notification en vue d'un contrôle préalable concernant les traitements réalisés dans le cadre des avis de sécurité sur les ressortissants de pays tiers accédant aux sites du Centre commun de recherche (ci-après, le «CCR»).

Le CCR a élaboré la procédure relative aux ressortissants de pays tiers en étroite collaboration avec la direction de la sécurité de la Commission (unité HR.DS.2), en réponse à deux événements:

- l'abolition de la procédure «nulla osta» du CCR (procédure d'habilitation) à compter du 1er septembre 2012[1], qui s'est traduite par une lacune dans la politique de sécurité du CCR concernant, entre autres éléments, le contrôle des ressortissants de pays tiers accédant à tous les sites du CCR, à l'exception de celui de Karlsruhe;
- l'instruction de la DG HR d'assurer sans délai le contrôle adapté des ressortissants de pays tiers accédant aux sites de la Commission.

À la suite de l'abolition de la procédure «nulla osta», la Commission a présenté une procédure de «contrôle de fiabilité» de sécurité du CCR (dossier 2012-1090) qui recouvre le traitement de données à caractère personnel de 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.

La procédure relative aux ressortissants de pays tiers a été mise en œuvre à partir du 1er septembre 2013, soit antérieurement à sa notification le 17 septembre 2013. En conséquence, l'analyse constitue un contrôle a posteriori d'un traitement.

Le 19 juin 2014, le projet d'avis du CEPD a été envoyé au DPD pour commentaires. Ces derniers ont été reçus le 7 juillet 2014.

[1] Décision du directeur général du CCR du 11 juillet 2012. Cette décision a résulté, en particulier, 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.

2. Faits

La ***finalité*** du traitement est de permettre à la hiérarchie du CCR de prendre une décision d'octroi ou de refus, à un ressortissant de pays tiers, d'une autorisation d'accès aux sites du CCR. La procédure relative aux ressortissants de pays tiers définit les circonstances dans lesquelles un contrôle de sécurité doit être effectué ainsi que les mesures préventives et les contre-mesures qui peuvent être mises en œuvre dans ce cadre. Le CCR entretient des relations de travail avec des établissements scientifiques de différents pays, qui peuvent supposer la présence sur les sites du CCR de personnel détaché de ces établissements et nécessitent souvent l'admission de visiteurs venus participer ou assister à des activités du CCR se déroulant sur ses sites. La spécificité des missions du CCR peut également nécessiter la présence sur les différents sites du CCR de sous-traitants externes (ou de soumissionnaires - au stade de la préparation et de la négociation d'un marché) qui fournissent des services commandés par le CCR. Nombre de ces personnes sont des ressortissants de pays tiers. Certains ressortissants de pays tiers sont des membres du personnel potentiels invités, par exemple, en vue d'entretiens de recrutement (comme des bénéficiaires de subventions, des visiteurs scientifiques, etc.).

La ***procédure*** comprend le traitement de données à caractère personnel au sens du règlement (CE) n° 45/2001 (ci-après, le «règlement»). Chaque membre du personnel du CCR formulant une demande d'accès d'un ressortissant de pays tiers à un site du CCR remplit un formulaire de demande qui contient toutes les données à caractère personnel pertinentes dans ce cadre (voir ci-après). Le service de sécurité local rend l'avis de sécurité sur la base des informations fournies. Avant de rendre l'avis, le service de sécurité local peut consulter la direction de la sécurité de la Commission (unité HR.DS.2). La décision d'accorder/de refuser l'accès sera adoptée par la hiérarchie du CCR sur le fondement de cet avis.

En ce qui concerne la ***base juridique***, le CCR a identifié les textes suivants:

- la décision de la Commission du 29 novembre 2001 - 2001/844/CE/CECA/EURATOM;
- la décision de la Commission relative aux niveaux d'alerte et à la gestion des situations de crise - décision de la Commission n° 2007/65/CE du 15 décembre 2006, en particulier la section 4 de l'annexe concernant le CCR;
- le protocole d'accord conclu entre la direction de la sécurité de la direction générale chargée des ressources humaines et de la sécurité («DG HR/DS») et le CCR concernant les tâches réalisées dans le domaine de la sécurité, Ares (2010)884864 - 30/11/2010;
- les «Mesures de sécurité liées à la présence de ressortissants de pays-tiers sans lien statutaire au sein de la Commission», Ares (2012)251857 - 16/11/2012.

Comme il a été observé dans le dossier 2012-1090, la Commission adoptera une nouvelle décision relative à la sécurité, sur le fondement de laquelle sera adopté un nouveau protocole d'accord entre la DG HR/DS et le CCR. Cette décision et ce protocole d'accord préciseront les compétences des différents services concernés et constitueront la base juridique des différents traitements, y compris de la procédure relative aux ressortissants de pays tiers. Aucun de ces documents n'a encore été adopté.

Le ***responsable du traitement*** est la Commission représentée par le directeur des ressources du CCR. Les sous-traitants des services de sécurité rattachés aux responsables de la sécurité locale de chaque site du CCR peuvent traiter les données en qualité de ***sous-traitants*** pour le compte du responsable du traitement.

Les ***personnes concernées*** sont des personnes physiques (et non des personnes morales, associations, fondations, etc.) ressortissants de pays tiers qui accèdent aux sites du CCR.

Les ***données traitées***, qui sont fournies par la personne concernée et accompagnées d'éléments de preuve sous forme papier, sont les suivantes:

- prénom, nom de famille, nationalité, numéro et date de délivrance du passeport, liste des pays visités au cours des 12 mois précédant la demande d'accès aux sites du CCR, motifs de la visite et durée du séjour dans ces pays, liste des sites du CCR déjà visités antérieurement à la demande de nouvel accès au(x) site(s) du CCR, motifs de la ou des visites et durée du séjour sur ces sites;
- documents contenant des données à caractère personnel: CV, extrait de casier judiciaire et avis du responsable de la sécurité locale des sites du CCR/de la direction de la sécurité de la DG HR.

Indépendamment des capacités du service de la sécurité et des outils utilisés sur les différents sites du CCR, les données sont traitées manuellement ou de manière informatisée en vue de la constitution d'un dossier se composant du formulaire de demande et de l'avis de sécurité sur le ressortissant de pays tiers.

S'agissant de la ***durée de conservation*** des données, la notification souligne que les sites du CCR sont soumis à la législation nationale qui impose différentes modalités en matière de conservation des données à caractère personnel des personnes accédant à leurs locaux, ces modalités dépendant également du niveau de sécurité de la zone à laquelle il est accédé. Conformément à la notification, les modalités suivantes s'appliquent:

- *Ispra*[2]: les opérations enregistrées dans le système de contrôle d'accès et les données relatives à des anomalies sont conservées pendant 24 mois; concernant l'accès à des zones contrôlées ou à des zones nucléaires, la durée de conservation est de 30 ans en raison d'exigences juridiques (par exemple, à des fins de conservation des données à caractère personnel concernant la dosimétrie d'exposition aux rayonnements, pour des motifs sanitaires);
- *Petten*[3]: les dossiers sont conservés pendant 3 mois. En cas d'incident, les données seront conservées pour analyse pendant une durée plus longue lorsque cela est nécessaire pour démontrer, exercer ou défendre un droit dans le cadre d'une action en justice en cours devant une juridiction;
- *Séville*[4]: les données relatives à l'identité et au *profil* d'accès du personnel statutaire sont conservées pendant toute la durée du contrat correspondant (c'est-à-dire associées à un badge d'accès du personnel valide); pour le personnel non statutaire, les données sont conservées pendant 24 mois. Les données relatives au *profil* d'accès des membres du personnel de sous-traitance externe sont conservées pendant toute la durée du contrat correspondant (c'est-à-dire associées à un badge d'accès du personnel valide). Les données relatives à l'accès sont conservées pendant 5 ans. Les données à caractère personnel des personnes participant à des ateliers/réunions (gérés par les unités scientifiques) sont associées au dossier de projet et sont conservées conformément aux exigences du projet. Le responsable de la sécurité en conserve une copie pendant une durée maximale de 6 mois après l'événement;
- *Geel*[5]: la durée de conservation est de 30 ans au minimum pour les zones de contrôle nucléaire et peut être ramenée à 5 ans sur demande pour les personnes qui n'ont pas accès aux zones de contrôle nucléaire;[6]

[2] DPO-2734.1 - JRC: système de contrôle de l'accès au site d'Ispra du CCR.
[3] DPO-1534.3 - JRC: système de gestion de l'accès au CCR-IE de Petten.
[4] DPO-1426.5 - JRC: contrôle de l'accès au CCR-IPTS de Séville.
[5] DPO-1177.6 - JRC: contrôle de l'accès au CCR-Geel.

– *Karlsruhe*[7]: les données à caractère personnel des membres du personnel et des sous-traitants seront supprimées 5 ans après la date d'expiration de l'habilitation de sécurité. Pour les visiteurs qui n'ont pas accès aux zones nucléaires, la durée de conservation maximale est de 5 ans après la dernière visite. Pour les personnes ayant accès aux zones nucléaires et dont les données dosimétriques ont été enregistrées, conformément à la notification, la durée de conservation maximale est de 95 ans à compter de la date de naissance de la personne concernée.[8]

Concernant les ***destinataires*** des données, le CCR établit une distinction entre les destinataires internes et externes:

– *destinataires internes*: les membres du personnel du CCR formulant une demande d'accès pour le ressortissant de pays tiers, leur hiérarchie, les responsables de la sécurité locale, le coordinateur de la sûreté et de la sécurité du CCR, la direction de la sécurité de la DG HR;
– *destinataires externes*: les sous-traitants chargés de la mise en œuvre et de la surveillance de la mise en œuvre des dispositions de sécurité (gardiens du site) - les informations fournies aux gardiens se limitent aux nom, prénom, numéro de passeport et décision d'autorisation d'accès (décision «access ok»). Le libellé de l'avis de sécurité et les informations comprises dans le formulaire de demande (autres que celles mentionnées ci-dessus) ne leur sont pas communiqués.

Concernant le ***droit à l'information***, le membre du personnel qui formule une demande d'accès au site du CCR pour le ressortissant de pays tiers adresse une Déclaration de confidentialité à chaque personne concernée par courrier électronique avant que le CCR ne commence à collecter les informations nécessaires pour remplir le formulaire. Ce document est également disponible sur demande et publié sur le site web du CCR. La Déclaration de confidentialité contient des informations sur la finalité du traitement (avec une brève description), les données à caractère personnel collectées, 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 (avec un renvoi au fait que la conservation des données à caractère personnel dépend de la législation nationale applicable à chaque site du CCR et du niveau de sécurité de la zone à laquelle il est accédé et l'indication d'un lien vers les durées de conservation de tous les sites). 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.

En ce qui concerne les ***droits d'accès et de rectification***, les personnes concernées peuvent exercer les droits suivants en envoyant un courrier électronique comportant une demande justifiée à une adresse de boîte de messagerie électronique fonctionnelle:

– le droit d'accès aux données à caractère personnel les concernant détenues par le responsable du traitement (à tout moment dans un délai de trois mois à partir de la réception de la demande et gratuitement, du responsable du traitement);

---

[6] La notification renvoie à l'article 30, paragraphe 1, de l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants, tel que modifié.

[7] DPO-1460.2 - JRC: autorisation d'entrée et contrôle d'accès à des fins de protection physique (ZES+ZKS) au CCR-ITU de Karlsruhe.

[8] La notification renvoie à l'article 42 du règlement allemand *Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung - StrlSchV)*, rédigé comme suit: «*Die Aufzeichnungen sind so lange aufzubewahren, bis die überwachte Person das 75. Lebensjahr vollendet hat oder vollendet hätte, mindestens jedoch 30 Jahre nach Beendigung der jeweiligen Beschäftigung. Sie sind spätestens 100 Jahre nach der Geburt der betroffenen Person zu löschen*».

– le droit de rectification des données à caractère personnel les concernant détenues par le responsable du traitement qui seraient inexactes ou incomplètes; les données seront corrigées ou modifiées dans un délai maximal de 14 jours.

En ce qui concerne les ***mesures de sécurité***,
[...]

3. Analyse juridique

3.1. Contrôle préalable

Le présent avis concerne le traitement de données à caractère personnel dans le cadre de la procédure relative aux ressortissants de pays tiers. 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 (CE) n° 45/2001, ci-après «le règlement»]. Le traitement de données à caractère personnel est effectué, à tout 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 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.

Le CEPD considère que ce traitement de données relève 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 se rapportant à des suspicions de délits ou à des condamnations pénales.

Le CEPD considère que, bien qu'il n'y soit pas renvoyé, la notification relève également de l'article 27, paragraphe 2, point b), du règlement, 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. En l'espèce, le comportement des personnes sera évalué afin de s'assurer de la possibilité d'accorder l'accès aux sites du CCR, déclenchant ainsi l'application de l'article 27, paragraphe 2, point b), du règlement, comme dans le cas de la procédure de «contrôle de fiabilité» de sécurité.[9]

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 traitement. En l'espèce, cependant, le traitement avait déjà été mis en place par la Commission. Il demeure que les recommandations émises par le CEPD doivent être pleinement mises en œuvre. La notification étant considérée comme une notification a posteriori, le délai de deux mois imparti au CEPD pour délivrer un avis conformément à l'article 27, paragraphe 4, du règlement ne s'applique pas à cette notification, qui a été traitée dans les meilleurs délais.

[9] Voir l'avis du CEPD du 19 juin 2013 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 (dossier 2012-1090).

3.2. 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.

Le CEPD considère que le traitement relève à la fois de l'article 5, point a), du règlement 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 (...)» et de l'article 5, point b), du règlement, dès lors que le traitement est nécessaire au respect d'une obligation légale à laquelle le CCR est soumis. En effet, la législation nationale des différents États membres prévoit des modalités différentes concernant les contrôles de sécurité des personnes physiques accédant aux sites du CCR situés sur leur territoire.[10] En particulier, cette législation nationale spécifique prévoit différentes durées de conservation des données à caractère personnel, comme décrit dans la partie relative aux faits.

Le CEPD prend note des actes législatifs de l'UE suivants[11], qui établissent certains motifs juridiques justifiant les traitements réalisés:

- la décision de la Commission relative aux niveaux d'alerte et à la gestion des situations de crise - décision de la Commission n° 2007/65/CE du 15 décembre 2006, en particulier la section 4 de l'annexe concernant le CCR;
- le protocole d'accord conclu entre la direction de la sécurité de la direction générale chargée des ressources humaines et de la sécurité («DG HR/DS») et le CCR concernant les tâches réalisées dans le domaine de la sécurité, Ares (2010)884864 - 30/11/2010, **lorsqu'il aura été mis à jour**;
- les mesures de sécurité liées à la présence de ressortissants de pays-tiers sans lien statutaire au sein de la Commission, Ares (2012) 251857) - 16/11/2012;
- en outre, la législation nationale imposant des mesures spécifiques fait partie de la base juridique, dès lors qu'elle impose la mise en œuvre de procédures spécifiques sur les sites du CCR.

Cependant, comme le CEPD l'a déjà indiqué dans le dossier relatif à la procédure de «contrôle de fiabilité» de sécurité (dossier 2012-1090)[12], la future décision de la Commission relative à la sécurité et le protocole d'accord entre la DG CCR et la DG HR mis à jour jouent un rôle crucial dans l'acquisition par le CCR de la capacité à mettre en œuvre ces procédures de sécurité. Ces deux textes garantiront également la légalité et la légitimité du traitement des avis de sécurité sur les ressortissants de pays tiers accédant aux sites du CCR. Tant que cette décision et le protocole d'accord n'auront pas été adoptés, la base juridique du traitement des données à caractère personnel ne saurait être considérée comme complète. **En conséquence, le CEPD recommande que la nouvelle décision de la Commission relative à la sécurité et le protocole d'accord mis à jour soient adoptés de toute urgence.**

[10] Comme il a été observé dans le dossier relatif à la procédure de «contrôle de fiabilité» de sécurité (dossier 2012-1090), à titre d'exemple, le site d'Ispra du CCR, en tant qu'opérateur nucléaire et titulaire d'une licence nucléaire conforme au droit italien, est soumis à des obligations spécifiques de mise en œuvre de nombreuses mesures de sécurité différentes.

[11] La décision C(2001)3031 de la Commission (aussi 2001/844/CE) mentionnée dans la notification n'est pas considérée comme pertinente en l'espèce.

[12] Dans son analyse du dossier 2012-1090, le CEPD avait déjà souligné la nécessité de fonder ces procédures liées à la sécurité sur la nouvelle décision relative à la sécurité et sur le protocole d'accord.

S'agissant de la nécessité du traitement, le CEPD relève que le traitement de données à caractère personnel dans le cadre de la procédure relative aux ressortissants de pays tiers est considéré comme nécessaire pour se conformer aux dispositions de l'UE et aux dispositions nationales applicables aux sites du CCR.

3.3. Traitement portant sur des catégories particulières de données

Compte tenu de la finalité du traitement, certains documents peuvent relever de l'article 10 du règlement. À cet égard, le CEPD souligne l'article 10, paragraphe 5, du règlement, 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, cette exception peut s'appliquer en raison des obligations légales auxquelles les sites du CCR sont soumis (voir les instruments juridiques mentionnés dans la partie relative aux faits et au point 3.2 ci-dessus).

3.4. Qualité des données

Conformément à l'article 4, paragraphe 1, point c), du règlement, 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 à caractère personnel traitées en l'espèce semblent limitées à ce qui est nécessaire pour répondre à la finalité de la procédure relative aux ressortissants de pays tiers et, partant, elles sont conformes à l'article 4, paragraphe 1, point c), du règlement.
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 des extraits de casier judiciaire, il convient de relever que la période pendant laquelle ces documents peuvent être considérés comme exacts est très limitée. Le CEPD invite donc le CCR à évaluer la nécessité de conserver un tel extrait au-delà d'une certaine période (voir également le point 3.5 ci-dessous).

3.5. Conservation/rétention des données

En vertu de l'article 4, paragraphe 1, point e), du règlement, 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 différentes durées de conservation en fonction de la législation nationale applicable à chaque site du CCR et du niveau de sécurité de la zone à laquelle il est accédé, comme décrit dans la partie relative aux faits. Au regard des informations fournies concernant la législation nationale applicable à chaque site du CCR, le CEPD ne voit aucun motif d'inquiétude concernant la nécessité et la proportionnalité des durées de conservation appliquées au regard de l'objectif poursuivi par la procédure relative aux ressortissants de pays tiers.
Toutefois, compte tenu de l'analyse ci-dessus, les données à caractère personnel contenues dans un extrait de casier judiciaire ne peuvent être considérées comme exactes que pendant une période extrêmement limitée. Le CEPD considère donc que la durée de conservation de l'extrait de casier judiciaire devrait être limitée à un maximum de deux ans après sa présentation. En effet, cela coïnciderait avec le délai durant lequel la Cour des comptes européenne vérifierait ce document (pour traitement ultérieur). Comme l'a accepté la Cour des

comptes européenne de manière formelle dans le dossier 2011-0482, les extraits de casier judiciaire ayant fait l'objet d'une vérification avant l'expiration de ce délai peuvent être détruits plus tôt. Le CEPD recommande de modifier la durée de conservation applicable aux extraits de casier judiciaire pour tenir compte de ce qui précède.

3.6. Traitement pour le compte du responsable du traitement

La procédure prévoit spécifiquement que les sous-traitants peuvent traiter des données pour le compte du responsable du traitement, puisque les sous-traitants des services de sécurité rattachés aux responsables de la sécurité locale de chaque site du CCR peuvent traiter des données pour le compte du responsable du traitement.
Le CEPD rappelle que le traitement de données à caractère personnel pour le compte du responsable du traitement doit être garanti par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et doit satisfaire aux exigences minimales suivantes prévues à l'article 23 du règlement: le contrat doit prévoir que le sous-traitant n'agit que sur instruction du responsable du traitement et le sous-traitant doit apporter des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives au traitement à effectuer et veiller au respect de ces mesures.
Le CEPD recommande donc au CCR de veiller à la satisfaction des exigences posées à l'article 23 et invite le CCR à lui fournir les documents correspondants.

3.7. Droits d'accès et de rectification

L'article 13 du règlement établit un droit d'accès et les modalités de son exercice à la demande de la personne concernée. Ce droit englobe celui d'être informé du fait que des informations la concernant font l'objet d'un traitement par le responsable du traitement et d'obtenir la communication de ces données sous une forme intelligible. L'article 14 du règlement accorde à la personne concernée un droit de rectification sans délai de données à caractère personnel inexactes ou incomplètes. La Déclaration de confidentialité mentionne une boîte de messagerie électronique fonctionnelle comme personne de contact pour exercer ces droits et prévoit que, sur demande justifiée soumise par l'intermédiaire de la boîte de messagerie électronique fonctionnelle, les données seront rectifiées ou modifiées dans un délai maximal de 14 jours. Le CEPD n'a aucun motif d'inquiétude concernant la conformité aux exigences posées aux articles 13 et 14 du règlement.

3.8. Information de la personne concernée

L'obligation d'informer les personnes concernées est consacrée par les articles 11 et 12 du règlement. Dans le cadre de la procédure relative aux ressortissants de pays tiers, la personne concernée se voit remettre une Déclaration de confidentialité préalablement à la collecte des informations nécessaires pour remplir le formulaire «ressortissants de pays tiers».
Le CEPD tient à observer que la Déclaration de confidentialité renvoie à des liens ou à des documents internes de la Commission ou du CCR dont les personnes concernées, qui peuvent ne disposer d'aucun accès direct à ces ressources, risquent de ne pas pouvoir prendre connaissance. À titre d'exemple, la Déclaration de confidentialité fournit des informations sur les législations nationales applicables à chaque site du CCR et les durées de conservation respectives en indiquant un simple lien vers le registre du DPD de la Commission. Le CEPD considère que la communication de ce lien vers le registre du DPD n'est pas suffisante pour assurer l'information correcte des personnes concernées, dès lors que celles-ci peuvent ne pas avoir accès à ce registre.
Le CEPD invite donc la Commission à veiller à ce que les informations sur les législations nationales applicables à chaque site du CCR et les durées de conservation respectives soient

fournies par un moyen plus aisément accessible aux personnes concernées. Il conviendra en outre d'introduire des renvois à la nouvelle décision de la Commission relative à la sécurité et au protocole d'accord mis à jour, une fois que ces textes auront été adoptés.
En ce qui concerne les autres éléments d'information fournis dans la Déclaration de confidentialité, le CEPD considère que celle-ci contient les informations requises au titre des articles 11 et 12 du règlement.

3.9. Mesures de sécurité

[...]

4. Conclusion

Le CEPD s'inquiète du fait que la nouvelle décision de la Commission relative à la sécurité, qui a été annoncée, et le protocole d'accord pertinent pour le présent traitement et celui examiné dans le dossier 2012-1090 n'aient pas encore été adoptés. Les deux documents présentent une grande importance en tant que base juridique de plusieurs traitements. Le CEPD souligne donc en particulier que tous les efforts doivent être faits pour que cette décision et ce protocole d'accord soient adoptés de toute urgence, en vue d'éviter toute lacune concernant la licéité des traitements concernés. **En conséquence, le CEPD demande instamment à la Commission d'adopter la nouvelle décision relative à la sécurité et le protocole d'accord dès que possible.**

La Commission doit tenir compte des recommandations suivantes. La Commission doit:

- veiller à ce que la nouvelle décision de la Commission relative à la sécurité et le protocole d'accord mis à jour soient adoptés de toute urgence et fournir ces documents au CEPD dès qu'ils seront disponibles;
- modifier la durée de conservation applicable aux extraits de casier judiciaire;
- veiller à ce que la Déclaration de confidentialité elle-même contienne des informations exhaustives;

[...]

Fait à Bruxelles, le 22 juillet 2014

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données