Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données du Conseil de l'Union européenne sur l'Accréditation du personnel des firmes externes participant aux réunions du Conseil européen

Bruxelles, le 16 septembre 2008 (Dossier 2007-046)

1. Procédure

Le 24 janvier 2007 une notification dans le sens de l'article 27 (2) du règlement (CE) n° 45/2001 (ci-après "le règlement") a été effectuée concernant le dossier "Accréditation du personnel des firmes externes participant aux réunions du Conseil européen".

Par e-mail en date du 9 février 2007, des questions sont posées au responsable du traitement par l'intermédiaire du délégué à la Protection des données du Conseil ("*DPD*"). Des réponses partielles sont fournies le 16 février 2007, le 26 février 2007 et le 5 novembre 2007. La procédure est restée suspendue jusqu'au 14 novembre 2007, jour où une réunion entre des agents du CEPD, le DPD du Conseil et le responsable du traitement a eu lieu. D'autres questions sont posées le 5 décembre 2007. Les réponses sont fournies en date du 18 juin 2008. Le projet d'avis a été envoyé au responsable du traitement le 11 juillet 2008 pour commentaires, qui ont été fournis le 15 septembre 2008.

2. Les faits

Finalité du traitement

La finalité du traitement est de permettre au Bureau de Sécurité du Secrétariat General ("*SGC*") du Conseil d'effectuer une appréciation en termes de sécurité[1] des prestataires de service ou des services de sécurité participants aux Sommets du Conseil Européen. Les personnes enregistrées pourront, le cas échéant, recevoir un badge leur octroyant l'accès au périmètre de sécurité établi autour du bâtiment dans lequel le Sommet a lieu. Il s'agit donc d'une base de données qui permet d'assurer l'enregistrement et le suivi des informations qui y sont reprises. Cette base permettra également d'assurer le suivi statistique des participants.

Personnes concernées

Les personnes concernées sont les prestataires de services en général et les services de sécurité (Police, Armée...).

[1] Voir la description des procédures de gestion de l'information, en ce qui concerne le "screening".

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.: 32-2-283 19 00 - Fax : 32-2-283 19 50

Catégories des données

Les données traitées sont les suivantes:

- information du badge

-Photo
-Numéro d'identification
-Badge (couleur/type)[2]
-Catégorie spéciale[3]
-Nom
-Prénom
-Société

- Accréditation

-Statut
-Attestation validité[4]
-Transfert vers la base AFTER[5]
-Délivrance du badge[6]
-Nom d'utilisateur
-Remarques[7]

- Information NSA (National Security Authority)

-Profession
-Date de naissance
-Lieu de naissance
-Nationalité
-Numéro de Registre National.
-Adresse
-Code postal
-Ville
-Pays

Informations destinées aux personnes concernées

[2] - badges rouges : donnent accès à la zone rouge.
- badges bleus : étage 50 jusqu'à la limite de la zone rouge.
- badges gris : destinés aux délégués techniques, personnel du SGC, firmes externes qui se trouvent aux étages 04, 03, 00, 10, 60 etc., accrédités spécifiquement pour le CE ou ayant leur bureau dans une zone de la partie Conférence du bâtiment. Un badge gris ne donne pas accès aux zones rouge ni bleu (sauf avec un floater bleu pour la zone bleue ou rouge pour la zone rouge)
- badges jaunes/verts : sécurité
- badgess verts : chauffeurs
- badges jaunes : presse
- floaters bleus : à porter avec un badge nominatif gris
- floaters rouges : à porter avec un badge nominatif bleu ou gris
- floaters or : à porter avec un badge nominatif rouge.

[3] D : Délégation ; I : Interprète ; T : Technicien; S: Securité.

[4] Délais de validité.

[5]. Indique que l'information a été transmise à l'entreprise qui produit les badges.

[6] Indique que la personne concernée a retiré son badge.

[7] Ce champ peut contenir de l'information opérationnelle. Le résultat du screening négatif est introduit dans ce champ.

En ce qui concerne les informations destinées aux personnes concernées, une note est jointe lors de l'impression de la demande d'attestation de sécurité concernant les informations ayant trait à la protection des données. La note contient les informations suivantes: l'identité du responsable; la finalité du traitement; les destinataires des données; le caractère obligatoire ou facultatif de la réponse aux questions ainsi que les conséquences éventuelles d'un défaut de réponse; l'existence d'un droit d'accès et de rectification; la base juridique du traitement; les délais de conservation des données et le droit de saisir à tout moment le Contrôleur européen de la protection des données.

Procédures garantissant les droits des personnes concernées

Lors des phases d'inscription de participation au Sommet, les personnes ont la possibilité de modifier les informations contenues sur leur fiche (accessible pour confirmation) via le responsable du service dont ils dépendent (voir ci-après la description des procédures de gestion de l'information). Dans tous les cas, ces informations sont contrôlées par le titulaire de la sollicitation lors de la signature de la demande d'attestation de sécurité (actuellement tous les 6 mois). En dehors de ces périodes, le Bureau de Sécurité est le seul responsable et autorisé à modifier ces données. Les droits des personnes concernées sont aussi garantis par la section 5 de la Décision du Conseil du 13 septembre 2004 portant adoption des dispositions d'application en ce qui concerne le règlement (CE) n° 45/2001.

Traitements automatisées / manuelles

La procédure est partiellement automatisée, toutes les créations des listes et leurs mises à jour sont automatisées. Les résultats de screening sont reçus par courrier officiel, donc ce traitement est effectué manuellement.

Description des procédures de gestion de l'information

La gestion des informations concernant le personnel des firmes externes ou services de sécurité lors des Sommets européennes, de réunions Extraordinaires ou Internationales, à des fins de contrôle de sécurité est faite de la façon suivante: les informations sont collectées depuis un formulaire sur un site sécurisé (HTTPS) sur l'Intranet. (...).

(...). L'administrateur du système crée alors automatiquement les listes de demandes de "screening". Les demandes de "screening" sont envoyées (...) aux différents services de sécurité (Autorité Nationale de Sécurité -ANS- belge ou ANS de la Présidence). Les listes créées à cet effet reprennent le nom, le prénom, la date de naissance et la nationalité et le cas échéant (par exemple pour la liste de l'ANS belge) le numéro de registre national. Les résultats sont communiqués aux responsables du système du Bureau de Sécurité d'abord par téléphone (par soucis d'efficacité) puis par courrier officiel. Pour les demandes concernant les services de sécurité (Police, Armée...), ces personnes ne sont pas soumises au "screening" et reçoivent l'accès automatiquement. Les résultats envoyés par les ANS se limitent au screening "positif" ou "négatif". Néanmoins, en vertu de la Décision du Secrétariat Général du Conseil No 198/03 (voir point 3.2 ci-après), le directeur du Bureau de Sécurité du Conseil peut en décider autrement, de façon exceptionnelle, durant la tenue d'un Sommet (ex: cas de comportement inadéquat).

Des informations sont communiquées à la société qui produit les badges. Les attestations de sécurité sont remises par les responsables des services au Bureau de Sécurité.

Ces données sont stockées sur un serveur dédié aux applications du Bureau de Sécurité du Secrétariat Général du Conseil de l'Union Européenne et gérées par la DGA 5 SIC.

Destinataires

Les destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées sont les suivants: (1) Administration : Personnel sélectionné de chaque Direction Générale ou service utilisateur de prestataire de service; (2) Screening : ANS belge pour les personnes résidentes en Belgique et le Service de Sécurité (ANS) de la Présidence[8] pour les personnes résidentes en dehors de la Belgique[9]; et (3) Création des badges : Société produisant les badges[10].

Sous-traitance

Le Conseil de l'Union européenne a signé un contrat avec une société qui produit les badges. La société est établie en Italie. Le contrat contient la mention suivante: "Le contractant s'engage à fournir 'des services d'accréditation et la fourniture de badges[11] correspondants', tels que définis dans l'annexe 2 (...) conformément aux dispositions du présent contrat"[12].

L'obligation de confidentialité est prévue à l'article 15 du contrat. Tandis que certaines mesures de sécurité sont établies à l'Annexe 2 du contrat.

---

[8] L'ANS du pays qui exerce la Présidence prend contact avec les pays de résidence des personnes concernées.

[9] Les données envoyées sont les suivantes : numéro de carte d'identité, prénom, nom, date de naissance, adresse, code postal, ville, pays, société, adresse de la société, code postal de la société, ville de la société, pays de la société.

[10] Les données envoyées sont les suivantes:

Header

ID|Photo|FirstName|LastName|Birthday|Sex|Org|Position|Type|ISO|Badge|CurrentSummit

Values

ID: ID of the external staff in our database. Always present.

Firstname: External staff first name. Always present, except for the floater badges: Red floater, Gold floater and Blue Floater

Lastname: External staff first name. Always present, except for the floater badges: Red floater, Gold floater and Blue Floater

Birthday: empty

Sex: empty

Org: Department within the Council where this person works (SGC - LOG, SGC - REST, MEDICAL, SCIC, etcetera).

Position: Name of the user requesting the badges.

Type: Badge type. Valid values: **I**, **S, T** and an empty string. Floater badges have no badge type.

ISO: empty

Badge: BLUE, GRAY, RED, GREEN, GREEN-YELLOW, Red Floater, Gold Floater, Blue Floater

CurrentSummit: Y

[11] Les badges contiennent une RFID. Le traitement issu de l'utilisation des badges ne fait pas objet du présent contrôle préalable.

[12] Article 1, 1.1. De l'anglais: Special Terms and Conditions: *"(...) The Contractor undertakes to provide 'Accreditation Services and supply of the corresponding badges' as defined in Annex 2 (...) in accordance with the provisions of this Contract"*.

Politique de conservation des données

Les données sont conservées pour une durée de 5 ans maximum. Le responsable du traitement a manifesté la volonté, à l'avenir, de conserver les données pendant 30 ans.

Date limite pour le verrouillage et l'effacement de différentes catégories des données

La date limite pour le verrouillage et l'effacement des différentes catégories de données (après requête légitime de la personne concernée) est d'une semaine.

Finalités historiques, statistiques ou scientifiques

Par ailleurs, certaines informations recueillies sont utilisées dans le but d'effectuer des statistiques par services et types de badges. Ces statistiques sont essentiellement utilisées par le Bureau de Sécurité. Ces statistiques sont strictement anonymes sans possibilité d'identification.

Mesures de sécurité

Des mesures de sécurité ont été prises.

3. Les aspects légaux

3.1. Contrôle préalable

L'accréditation du personnel des firmes externes participant aux réunions du Conseil européen constitue un traitement de données à caractère personnel (*"toute information concernant une personne physique identifiée ou identifiable (...)"* article 2.a du règlement (CE) 45/2001). Le traitement de données présenté est effectué par une Institution et est mis en œuvre pour l'exercice d'activités relevant du champ d'application du droit communautaire.

Les données sous analyse sont traitées de façon tant automatisée que manuelle. Elles sont donc constitutives d'un traitement partiellement automatisé (article 3.2 du règlement).

Dès lors, ce traitement tombe sous le champ d'application du règlement (CE) 45/2001.

L'article 27.1 du règlement (CE) 45/2001 soumet au contrôle préalable du CEPD les traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées. L'article 27.2 contient une liste de traitements susceptibles de présenter semblables risques. L'article 27.2.a présente comme traitements susceptibles de présenter de tels risques *"les traitements de (...) données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté"*. .

La procédure d'accréditation du personnel des firmes externes participant aux réunions du Conseil européen implique un traitement de données à caractère personnel entrant dans le cadre de l'article 27.2.a et, à ce titre, est soumis au contrôle préalable du CEPD. En effet l'article 27.2.a est applicable dans la mesure où un résultat "négatif" du screening peut être

vraisemblablement assimilé à une donnée relative à des suspicions, infractions, condamnations pénales ou mesures de sûreté.

Des lors, même si l'article 27.2.b a été mentionné dans le formulaire de notification, le CEPD a été informé que le responsable du traitement ne fait aucune évaluation *"des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement"*, dans le contexte du traitement de données sous analyse.

En principe, le contrôle effectué par le CEPD est préalable à la mise en place du traitement. Dans ce cas, en raison de la nomination du CEPD, qui est postérieure à la mise en place du système, le contrôle devient par la force des choses *ex-post*. Ceci n'enlève rien à la mise en place souhaitable des recommandations présentées par le CEPD.

La notification a été reçue le 24 janvier 2007. Conformément à l'article 27, paragraphe 4, le présent avis doit être rendu dans les deux mois. Ce délai a été suspendu pour une durée de 502 jours (+ 2 moins d'août).pour commentaires. Le CEPD rendra son avis au plus tard pour le 17 septembre 2008.

3.2. Licéité du traitement

La licéité du traitement doit être examinée à la lumière de l'article 5.a du règlement (CE) 45/2001 qui prévoit que *"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 (...) ou relevant de l'exercice légitime de l'autorité publique dont est investie l'institution"*.

L'appréciation en termes de sécurité des participants aux Sommets du Conseil Européen est une mission effectuée dans l'intérêt public.

Cette mission est effectuée en ayant comme base légale l'article 23 de la Décision du Conseil du 15 septembre 2006 portant adoption de son règlement intérieur[13], à savoir: *"2. Le Conseil décide de l'organisation du secrétariat général. Sous son autorité, le secrétaire général et le secrétaire général adjoint prennent toutes les mesures nécessaires pour assurer le bon fonctionnement du secrétariat général"*.

De plus, la Décision 198/03 du Secrétaire Général du Conseil / Haut représentant pour la politique étrangère et de sécurité commune concernant les tâches du Bureau de Sécurité, établit:

Article 2
"Le Bureau de sécurité a pour mission d'assurer la protection des personnes, des bâtiments, des biens, des activités et des informations classifiées ou sensibles contre tout acte violent ou malveillant, dans les lieux où se déroulent normalement les travaux du Conseil et de son Secrétariat général.

Le Bureau de sécurité coordonne, supervise et met en oeuvre toutes les mesures de sécurité, conformément au règlement de sécurité du Conseil de l'Union européenne (ci-après dénommé "règlement de sécurité"). Il est le principal conseiller du Secrétaire général/Haut

[13] JOCE L 285, 16.10.2006, p. 47.

représentant et du Secrétaire général adjoint pour tous les problèmes ayant trait à la sécurité.(...)".

Article 4
"Lorsqu'ils exécutent les tâches du Bureau de sécurité, ses agents peuvent, en cas de besoin et conformément au règlement de sécurité:
- vérifier l'identité de toute personne souhaitant pénétrer dans l'un des bâtiments du Conseil ou dans l'un des lieux où se déroulent ses travaux et, le cas échéant, en refuser l'accès à cette personne;
- inspecter les bagages des personnes à l'entrée, à la sortie, ou pendant le séjour à l'intérieur des bâtiments du Conseil ou des lieux où se déroulent ses travaux, et refuser l'accès aux personnes qui n'acceptent pas de se soumettre à ces inspections;
- vérifier l'identité de toute personne se trouvant dans les locaux du Conseil ou dans les lieux où se déroulent ses travaux et, lorsque cela se justifie, en faire sortir les personnes qui ne détiennent pas d'autorisation d'accès appropriée ou qui troublent l'ordre public;
- inspecter le contenu des véhicules à moteur à l'entrée et à la sortie des bâtiments du Conseil ou pendant leur séjour dans l'enceinte du Conseil, ou refuser l'accès aux conducteurs qui n'acceptent pas de se soumettre à cette inspection, ainsi qu'à leurs véhicules.".

La base légale est donc conforme et vient à l'appui de la licéité du traitement.

Par ailleurs, le traitement décrit est nécessaire pour l'accomplissement de la mission.

3.3. Traitement portant sur des catégories particulières de données

Comme mentionné dans le point 2, une des données traitées est la photographie de la personne concernée. Cette donnée peut révéler l'origine raciale ou ethnique de l'individu. Par conséquent, le traitement doit être analysé à la lumière de l'article 10.1 du règlement. En effet, le traitement de données à caractère personnel relatives à l'origine raciale ou ethnique est interdit, à moins qu'un tel traitement ne soit justifié par une des exceptions des paragraphes suivants.

Dans le cas d'espèce, l'article 10.2(a) (consentement de la personne concernée) pourrait être applicable dans le cas des travailleurs indépendants qui demandent l'accréditation. Cependant, cet exception ne pourrait pas être d'application dans le cas des employés des firmes externes car s'est l'employeur qui prend la décision de demander l'accréditation et donc le consentement du travailleur ne peut pas être considéré, en principe, comme étant "libre" (voir la définition du "consentement de la personne concernée" établie par l'article 2(h)). De plus, aucune des exceptions prévues à l'article 10.2 n'est applicable à ces travailleurs. Néanmoins, le CEPD considère qu'il s'agit d'un traitement nécessaire pour un motif d'intérêt public important, et donc ce traitement doit être autorisé à la lumière de l'article 10.4 du règlement. Des garanties appropriées protégeant cette information ont été adoptées.

Enfin, l'article 10.5 est respecté dans le cas sous analyse (voir point 3.2).

3.4. Qualité des données

"Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement" (article 4.1.c du règlement).

Les données traitées dans le cadre de l'accréditation du personnel des firmes externes participant aux réunions du Conseil Européen, décrites dans le point 2 de cet avis, respectent ce principe.

Par ailleurs, les données doivent être *"traitées loyalement et licitement"* (article 4.1.a du règlement). La licéité a déjà fait l'objet d'une analyse dans le point 3.2 de cette opinion. Quant à la loyauté, elle est liée aux informations qui doivent être transmises à la personne concernée (voir ci-dessous point 3.9).

Enfin, les données doivent être *"exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées"* (article 4.1.d du règlement).

Le système tel que décrit ci-dessus permet raisonnablement de penser que les données sont exactes et mises à jour. Les droits d'accès et de rectification sont à la disposition de la personne concernée. Ils représentent la deuxième possibilité d'assurer la qualité des données (concernant les droits d'accès et de rectification, voir point 3.8 ci-après).

3.5. Conservation des données

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. (...)"* (article 4.1.e du règlement).

Pour mémoire, la durée de conservation des données est de 5 ans. Le responsable du traitement a manifesté la volonté de conserver, à l'avenir, les données pendant 30 ans. La durée de 5 ans est proportionnée. Quant à l'extension de cette durée, elle doit être l'objet d'une évaluation plus approfondie. Si le risque d'attentat terroriste pourrait justifier une extension de la durée, les éléments permettant d'établir la proportionnalité d'une durée de 30 ans n'ont pas été apporté. Le CEPD demande qu'une durée proportionnelle soit fixée, eu égard à la finalité du traitement et aux conditions de mise en place du traitement envisagées.

3.6. Transfert des données

Transferts des données entre institutions ou organes communautaires ou en leur sein

Le traitement doit également être examiné à la lumière de l'article 7.1 du règlement. Le traitement au regard de l'article 7.1 concerne les transferts de données à caractère personnel entre institutions ou organes communautaires ou en leur sein "*si nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire*".

Comme indiqué plus haut, des données sont envoyées au personnel sélectionné de chaque Direction Générale ou au service utilisateur du prestataire de service pour la finalité d'exécution des taches administratives.

L'article 7.1 du règlement est respecté, car les transferts sont nécessaires à l'exécution légitime de missions relevant de la compétence des destinataires.

Enfin, l'article 7.3 du règlement stipule que "*le destinataire traite les données à caractère personnel uniquement aux fins qui ont motivé leur transmission*". C'est pourquoi le CEPD recommande que toute personne recevant et traitant des données dans le cadre présent soit informée qu'elle ne pourra pas les utiliser à d'autres fins.

Transferts de données à des destinataires autres que les institutions et organes communautaires et relevant de la Directive 95/46/CE

Par ailleurs, des données sont transférées à la société qui est chargée de la création des badges. Cette société est un destinataire relevant de la législation nationale adoptée en application de la directive 95/46/CE. En l'occurrence ce transfert sera couvert par l'article 8.a du règlement qui indique que le transfert est possible si "*le destinataire démontre que les données sont nécessaires à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique*".

En effet, la société qui produit les badges traite les données pour le compte du Conseil dans le cadre de la mission décrite ci-dessus, qui est effectuée dans l'intérêt public. Etant donné que, en l'espèce, les données ne sont pas demandées par le destinataire, mais que le transfert est décidé unilatéralement par le responsable du traitement, ce dernier doit établir la "nécessité" du transfert. La "nécessité" du traitement aux fins de l'accomplissement de la mission du Conseil a été établie au point 3.2.

Le CEPD constate avec satisfaction que le transfert des données est fait de façon sélective, c'est à dire, que la société ne reçoit que les données nécessaires pour remplir sa tâche.

Transfert de données à des destinataires autres que les institutions et organes communautaires et ne relevant pas de la directive 95/46/CE

Des donnés sont aussi transférées à l'ANS belge et à l'ANS du pays qui exerce la Présidence pour le "screening" des personnes. L'article 9 du règlement stipule: *"1. Le transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires, et qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, ne peut avoir lieu que pour autant qu'un niveau de protection adéquat soit assuré dans le pays du destinataire ou au sein de l'organisation internationale destinataire, et que ce transfert vise exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement".*

En effet, les ANS ne sont pas soumis à la directive 95/46/CE, et donc, le transfert décrit doit respecter l'article 9. Dans cette optique, deux prémisses doivent être analysées: (1) si la protection assurée par les ANS peut être considérée comme octroyant un niveau de protection adéquat; (2) si ce transfert vise exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement.

En premier lieu, même si les ANS ne sont pas soumis à la Directive 95/46/EC, elles sont soumises à la Convention du Conseil de l'Europe No 108[14], ce qui fait que, en principe, le niveau de protection puisse être considéré comme adéquat.

En deuxième lieu, le transfert est effectué afin de permettre au Bureau de Sécurité du Conseil de l'Union européenne l'exécution d'une mission qui relève de sa compétence, à savoir, la réalisation d'une appréciation en termes de sécurité des prestataires de service ou des services de sécurité participants aux Sommets.

Le CEPD considère, par conséquence, que l'article 9 est respecté.

3.7. Traitement incluant le numéro de personnel ou le numéro identifiant

L'article 10.6 stipule: *"[L]e contrôleur européen de la protection des données détermine les conditions dans lesquelles un numéro personnel ou tout autre identifiant utilisé de manière générale peut faire l'objet d'un traitement par une institution ou un organe communautaire"*.

Le Conseil utilise un numéro identifiant pour le traitement sous analyse (numéro d'identification). Ce numéro est ensuite transmis à l'entreprise qui produit les badges. Il ne s'agit pas ici d'établir les conditions dans lesquelles le Conseil peut traiter ce numéro mais de souligner l'attention qui doit être portée à ce point du règlement. En l'espèce, l'utilisation du numéro est raisonnable car l'utilisation s'effectue à des fins d'identification de la personne et de suivi de la procédure d'accréditation.

3.8. Droit d'accès et de rectification

L'article 13 du Règlement dispose du droit d'accès - et de ses modalités - à la demande de la personne concernée par le traitement. L'article 14 du Règlement dispose du droit de rectification pour la personne concernée.

En l'espèce, chaque personne peut accéder à ses données en s'adressant au responsable du traitement. Elle peut également en demander la rectification. Ces droits sont indiqués dans les notices informatives remises aux personnes concernées.

3.9. Information des personnes concernées

Le règlement prévoit que la personne concernée doit être informée lorsqu'il y a traitement de ses données personnelles et énumère une série de mentions obligatoires dans cette information.

Les dispositions de l'article 11 (*Informations à fournir lorsque les données sont collectées auprès de la personne concernée*) sur l'information de la personne concernée sont applicables en l'espèce. Dans la mesure où la personne concernée remplit des formulaires, les données sont fournies par elle-même.

---

[14] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28.I.1981.

Les dispositions de l'article 12 (*Informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée*) sur l'information de la personne concernée sont aussi applicables en l'espèce, car les résultats du "screening" sont fournis par les ANS.

Pour mémoire, l'information des personnes concernées est assurée dans le cas présent par le biais de la note informative jointe lors de l'impression de la demande d'attestation de sécurité.

Le CEPD note que la base légale du traitement présent n'est pas le consentement, et donc, la référence "Il importe de remarquer que les candidats donnent ces données sur base volontaire et que nul n'est obligé de les donner", ne doit pas être inclus dans la note d'information. En effet, les personnes qui demandent l'accréditation sont, en général, des employés de firmes privées ou de l'Etat, et par conséquent, le champ d'application du consentement dans le cadre des relations de travail est réduit, et, en tout cas, n'est pas applicable en principe au cas d'espèce, sauf pour les travailleurs indépendants.

Par ailleurs, le CEPD signale que la base légale doit être corrigée à la lumière du présent avis (voir la base légale mentionné au point 3.2)..

3.10. Traitement de données pour le compte du responsable du traitement

Dans le cas présent, la création des badges d'accès est faite par une société sous-traitante qui, à cet effet, reçoit les données mentionnées au point 2 *supra*.

Lorsqu'une opération de traitement est effectuée pour le compte d'un responsable du traitement, l'article 23 du règlement stipule que celui-ci choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation prévues par le règlement. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur instruction du responsable du traitement et que les obligations de confidentialité et de sécurité concernant le traitement des données à caractère personnel incombent également au sous-traitant.

La clause 1 mentionné au point 2 *supra* permet déduire que le sous-traitant n'agit que sur instruction du responsable du traitement, car il fournit les services comme établi à l'annexe 2 du contrat.

Le CEPD signale néanmoins, que l'introduction d'un addendum a la clause 16 du contrat est nécessaire pour clarifier le fait que non seulement les données inclues dans le contrat doivent être traitées en respectant le règlement 45/2001 mais aussi toutes les données personnelles qui sont traitées lors de l'exécution du contrat. De plus, l'addendum doit signaler que la loi applicable à l'obligation de confidentialité et de sécurité est la loi italienne.

3.11. Sécurité

Conformément à l'article 22 du Règlement relatif à la sécurité des traitements, *"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"*.

Au regard de l'ensemble des mesures de sécurité prises, le CEPD estime que celles-ci peuvent être considérées comme adéquates au sens de l'article 22 du règlement.

Conclusion

Le traitement proposé ne paraît pas entraîner de violations des dispositions du règlement (CE) 45/2001 pour autant qu'il soit tenu compte des observations faites ci-dessus. Cela implique, en particulier, que :

- une durée de conservation proportionnelle reste retenue, eu égard à la finalité du traitement.
- toute personne recevant et traitant des données dans le cadre présent soit informée qu'elle ne pourra pas les utiliser à d'autres fins.
- la référence "Il importe de remarquer que les candidats donnent ces données sur base volontaire et que nul n'est obligé de les donner", ne soit pas inclue dans la note d'information.
- la base légale soit corrigée à la lumière du présent avis dans la note d'information (article 23 de la Décision du Conseil du 15 septembre 2006, et Décision 198/03 du SGCl / Haut représentant pour la politique étrangère et de sécurité commune)
- un addendum à la clause 16 du contrat soit ajouté pour clarifier le fait que non seulement les données inclues dans le contrat doivent être traitées en respectant le règlement 45/2001 mais aussi toutes celles qui sont traitées lors de l'exécution du contrat. De plus, l'addendum doit signaler que la loi applicable à l'obligation de confidentialité et de sécurité est la loi italienne.

Fait à Bruxelles, le 16 septembre 2008

(signé)

Joaquín BAYO DELGADO
Contrôleur européen adjoint de la protection des données