To be filled out in the EDPS' office

NUMERO DE REGISTRE: 146

NOTIFICATION DE CONTRÔLE PREALABLE

Date de soumission : 24 janvier 2007

Numéro de dossier : 2007-046

Institution : Conseil de l'Union européenne

Base légale : article 27-5 du Règlement CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATIONS NECESSAIRES (2)

(2) Merci de joindre tout document utile

1/ Nom et adresse du responsable du traitement

Legein Alexandro
Directeur du bureau de Sécurité
Services rattachés au SG/HR – SGA
Bureau de Sécurité
Conseil de l'Union européenne
Rue de la Loi 175
1048 Bruxelles
Tél : +32 2 281 85 17
Fax +32 2 281 73 97

2/ Services de l'institution ou de l'organe chargés du traitement de données à caractère personnel

Bureau de Sécurité

3/ Intitulé du traitement

Accréditation du personnel des firmes externes participant aux réunions du Conseil Européen

4/ La ou les finalités du traitement

Cette base de données permet d'assurer l'enregistrement et le suivi des informations qui y sont reprises. Elle permet au Bureau de Sécurité d'effectuer une appréciation en terme de sécurité des prestataires de service ou des services de sécurité participants aux Sommets. 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. Cette base permettra également d'assurer le suivi statistique des participants.

5/ Description de la categorie ou des categories de personnes concernées

Prestataires de services, service de sécurité (Police, Armée...)

6/ Description des données ou des catégories de données *(en incluant, si nécessaire, les catégories particulières de données (article 10) et/ou l'origine des données)*

Voir Annexe 1

7/ Informations destinées aux personnes concernées

Les responsables des services sont informés de la procédure pour la demande de badges par une note du Bureau de Sécurité qui est diffusée à toutes les DGs pour information et explication (Annexe 3) .
Concernant les personnes résidantes en Belgique ou de Nationalité Belge, une impression automatique de l'attestation de sécurité pré remplie se fait le cas échéant (nouvelle inscription ou période de validité expirée). (Annexe 2).
Ce document doit être par ailleurs signé, puis être remis à l'accréditation du Bureau de Sécurité du Conseil pour pouvoir recevoir le cas échéant une carte d'accès. Ce document est ensuite envoyé par le bureau de sécurité du Conseil à la direction générale centre de crise du SPF intérieur, 53 rue Ducale 1000 Bruxelles pour "screening". Lorsque le résultat du "screening" est connu, les personnes sont informées, par le responsable du service pour lequel la prestation est demandée, les indiquant la marche à suivre.

Pas d'application pour les membres des services de sécurité. Par ailleurs, une information est jointe lors de l'impression de la demande d'attestation de sécurité concernant les informations ayant trait à la protection des données. (Annexe 4).

8/ Procédures garantissant les droits des personnes concernées*(droits d'accès, de faire rectifier, de faire vérouiller, de faire effacer, d'opposition)*

Section 5 de la Décision du Conseil du 13.9.2004: 2004/644/CE (JO L n° 296, 21.9.2004, p.20)

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. 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.

Voir

- ANNEXE 2 Texte d'autorisation ou de non soumission à la demande de l'attestation de sécurité

- ANNEXE 3 Note au DG

9/ Procédures de traitement automatisées / manuelles

Procédure partiellement automatisée, Toutes les créations des listes et leurs mises à jour sont automatisées. Tous les envois se font manuellement.

Management des informations concernant le personnel des firmes externes ou services de sécurité lors de Sommet Européen, de réunions Extraordinaires ou Internationales à des fins de contrôle de sécurité. - Les informations sont collectées depuis un formulaire sur un site sécurisé (HTTPS)sur Intranet. - Grâce à un login et un mot de passe, le responsable désigné par service encode les données de chaque personne depuis un site et via un lien sécurisé sur Intranet. - Ces données sont stockées sur un serveur dédié aux applications du Bureau de Sécurité du Secrétariat Général du Conseil de l'Union Européenne situé dans un local protégé et dont l'accès est limité. - Ces informations ne sont accessibles qu'à un nombre limité d'utilisateurs du SGC via un identifiant (logins et mots de passe). Listes de ces utilisateurs : Les 4 responsables du système au Bureau de Sécurité (droit administration) Les administrateurs du système de la DGA 5 CIS (droit administration) Les responsables de chaque service désignés (droit utilisateur).
Chaque service ne peux consulter que la liste de son service '- Par ailleurs, un outil de nettoyage et de correction des données (mauvaise photo ou de mauvaise qualité) est utilisable uniquement par les 4 responsables du système du Bureau de Sécurité. '- L'administrateur du système crée alors automatiquement les listes de demandes de "screening". '- Les demandes de "screening" sont envoyées par courrier électronique aux différents service de sécurité (ANS belge ou de la Présidence). Les listes créées à cet effet reprennent le nom, le prénom, la date de naissance et la nationalité et pour la liste pour de la ANS belge, le cas échéant 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 automatiquement accès.
- Les demandes de "screening" sont envoyées par courrier électronique aux différents services de sécurité. '- Les listes créées à cet effet reprennent le nom, le prénom, la date de naissance et la nationalité de la personne. '- Les résultats sont communiqués aux responsables du système au Bureau de sécurité d'abord par téléphone (par soucis d'efficacité) puis par courrier officiel. - Les informations tel que le nom, le prénom, le société, la couleur du badge, la photo et la nationalité de la personne sont communiquées à la société qui produit les badges. '- Les attestations de sécurité sont remises par les responsables des services au Bureau de Sécurité. '- Les attestations sont ensuite envoyées au Centre de crise du Service Public Fédéral Intérieur.

10/ Support de stockage des données

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

11/ Base légale et licéité du traitement
- Articles 5 et 23 du règlement de sécurité du Conseil - Annexe à l'arrêté Royal du 3 Juin 2005 modifiant l'Arrêté Royal du 24 Mars 2000 portant exécution de la loi du 11 Décembre 1998 relative à la classification et aux habilitations de sécurité.

Article 5, point (a) et (b) de (EC) Regulation No 45/2001

12/ Destinataires ou categories de destinataires auxquels les données sont susceptibles d'être communiquées
Administration : Personnel sélectionné du Bureau de Sécurité et de chaque Direction Générale ou service utilisateur de prestataire de service. Screening : ANS belge pour les personnes résidentes en Belgique. Service de Sécurité de la Présidence pour les personnes résidentes en dehors de la Belgique. Consultation : Bureau de Sécurité du Conseil de l'UE. Création des badges : Société produisant les badges.

13/ Politique de conservation des données personnelles (ou catégories de données)
- Durée de 5 ans maximum - Attestation de sécurité délivrée par l'Etat Belge ou validité du "screening". Durée du 1/01 au 30/06 de la même année pour les attestations de sécurité demandées durant cette période et du 01/07 au 31/12 pour les attestations de sécurité demandées durant cette période.

13 a/ Dates limites pour le verouillage et l'effacement des différentes catégories de données (après requête légitime de la personne concernée)
(Merci d'indiquer les dates limites pour chaque catégorie, si nécessaire)
Une semaine.

14/ Finalités historiques, statistiques ou scientifiques
Si vous conservez les données pour des périodes plus longues que celles mentionnées ci-dessus, merci d'indiquer, si nécessaire, ce pourquoi les données doivent être conservées sous une forme permettant l'identification.
Certaines informations recueillies sont utilisées dans le but d'effectuer des statistiques par service, et types de badges. Ces statistiques sont essentiellement utilisées par le Bureau de Sécurité. Ces statistiques sont strictement anonymes sans possibilité d'identification.

15/ Transferts de données envisagés à destination de pays tiers ou d'organisations internationales
Néant

16/ Le traitement présente des risques particuliers qui justifient un contrôle préalable :*(Merci de décrire le traitement)* :
Le Secrétariat Général du Conseil n'est pas tenu par les décisions d'octroi ou non des attestations de sécurité. Dès lors,le Bureau de Sécurité peut être appelé à effectuer une évaluation de l'aspect de la personnalité des personnes concernées. Article 27.2 a), b) et d)

comme prévu à:

Article 27.2.(a) **X**
Les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté,

Article 27.2.(b) **X**
Les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement,

Article 27.2.(d) **X**

Les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.

17/ Commentaires

Néant
LIEU ET DATE: Bruxelles, le 22 janvier 2007 DELEGUE A LA PROTECTION DES DONNEES: Pierre Vernhes INSTITUTION OU ORGANE COMMUNAUTAIRE: Conseil de l'Union européenne