

JOAQUIN BAYO DELGADO
CONTRÔLEUR ADJOINT

M. Spyros ANTONIOU
Délégué à la protection des données
CEDEFOP
PO Box 22427
55102 Thessalonique
Grèce

Bruxelles, le 2 septembre 2008
JBD/DH/ktl D(2008)1163 C 2008-0195

Cher Monsieur Antoniou,

Je me réfère à la notification en vue d'un contrôle préalable relatif au traitement des données à caractère personnel dans le cadre du "contrôle de l'accès aux locaux" (2008-195)¹.

Ayant examiné le contenu de la notification ainsi que ses annexes, nous sommes arrivés à la conclusion que **ce type de traitement n'est pas soumis au contrôle préalable** au titre de l'article 27 du règlement (CE) n° 45/2001 (ci-après dénommé "le règlement").

L'article 27, paragraphe 1, du règlement soumet au contrôle préalable du contrôleur européen de la protection des données (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 énumère les traitements susceptibles de présenter des risques particuliers au sens susvisé. La notification en vue d'un contrôle préalable a été présentée au titre de l'article 27, paragraphe 2, point a) du règlement.

Aux termes de l'article 27, paragraphe 2, point a), du règlement, les traitements de données relatives à la santé et à des suspicions, infractions, condamnations pénales ou mesures de sûreté présentent un risque particulier. Selon l'interprétation du CEPD, les "mesures de sûreté" visées à l'article 27, paragraphe 2, point a), ne portent pas sur la protection physique des bâtiments et du personnel mais désignent plutôt les mesures prises à l'égard des personnes physiques dans le cadre de procédures pénales (ou administratives).

Nous avons également examiné si d'autres aspects du traitement nécessitaient un contrôle préalable. L'utilisation de la technologie RFID est un aspect important à cet égard. Le CEPD considère que la RFID en elle-même, sans autre élément additionnel, ne présente pas de risques particuliers au sens de l'article 27, paragraphe 1. Cela ne signifie toutefois pas qu'il n'est pas nécessaire de recommander d'utiliser les meilleures pratiques afin de garantir le respect de la vie privée et la protection des données. Tel est le cas en l'espèce (voir ci-après).

¹ Le CEPD est conscient du fait que les locaux comprennent la garderie; voir l'avis du CEPD sur le dossier 2008-193.

Pour conclure, nous estimons que le traitement ne justifie pas un contrôle préalable, à moins que vous ne nous fournissiez des éléments spécifiques nous amenant à revoir notre décision.

Recommandations et suivi:

Bien qu'ils ne doivent pas faire l'objet d'un contrôle préalable, le CEPD souhaiterait néanmoins attirer votre attention sur les aspects suivants:

- la finalité du traitement n'est pas clairement indiquée dans la notification. Les explications fournies dans les encadrés 4, 9, 12 et 13 manquent de clarté; il est fait état de deux traitements différents: le contrôle d'accès et la gestion du temps (Flexitime). Le système Flexitime, tel qu'il est mentionné dans votre courrier électronique du 21 avril 2008, devrait faire l'objet d'une notification distincte en vue d'une consultation quant à la nécessité d'un contrôle préalable du CEPD. En conséquence, pour éviter toute confusion, il conviendrait dans le futur d'établir cette distinction dans la notification et dans l'information des personnes concernées;
- la notification devrait comprendre une description du contrôle de l'accès interne;
- le CEPD a reçu uniquement la déclaration de confidentialité destinée aux visiteurs. Il considère que les informations prévues aux articles 11 et 12 du règlement devraient être communiquées aux membres du personnel du Cedefop, puisqu'ils sont également concernés par le traitement de données. Les informations fournies aux personnes concernées constituent en effet une des conditions d'un traitement loyal;
- en ce qui concerne la conservation des données, le CEPD recommande une période qui ne soit pas plus longue que nécessaire aux fins du contrôle de l'accès, c'est-à-dire trois mois maximum;
- le Cedefop a mis en circulation, aux fins du contrôle de l'accès, une carte HID appelée "MiniProx". Elle a une distance de lecture de 14 cm et comporte un numéro d'identification unique. Le CEPD recommande d'assurer une meilleure protection du respect de la vie privée et de la protection des données en veillant à ce que le badge ne puisse pas être copié et à ce qu'on ne puisse pas suivre les déplacements de son détenteur. Des technologies plus appropriées, telles que des cartes à puce sans contact utilisant un numéro d'identification aléatoire, pourraient être choisies et appliquées². Une autre solution serait que le Cedefop utilise une protection plus solide pour la carte (feuille d'aluminium), qui serait retirée uniquement lors de son utilisation. Ces mesures techniques devraient être complétées par des procédures telles que: i) interdiction de partager ou de prêter les cartes d'accès, ii) signalement immédiat du vol ou de la perte des cartes d'accès et iii) recommandation aux membres du personnel de cacher leur carte d'accès lorsqu'ils ne se trouvent pas dans les locaux du Cedefop.

Nous vous prions d'informer le CEPD dans un délai de trois mois des mesures adoptées à la suite des recommandations formulées dans la présente lettre.

Nous restons bien évidemment à votre disposition pour toute nouvelle consultation sur cette question.

(Formule de politesse)

Joaquín BAYO DELGADO

² Cette question a été soulevée l'année dernière par l'Organisation de l'aviation civile internationale (OACI), voir page 22:
http://www.mrtd.icao.int/component/option,com_remository/Itemid,256/func,startdown/id,26/