EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
CONTRÔLEUR ADJOINT

M. Udo HELMBRECHT
Directeur exécutif
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)
P.O. Box 1309
710 01 Héraklion,
Crête
GRÈCE

Bruxelles, le 31 mars 2016
WW/XK/sn/D(2016)0756 **C 2011-1149**
Veuillez utiliser l'adresse edps@edps.europa.eu pour toute correspondance.

Objet: **Avis de contrôle préalable concernant le traitement des données relatives à la santé au sein de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (dossier 2011-1149)**

Monsieur,

Le 15 décembre 2015, le Contrôleur européen de la protection des données (CEPD) a reçu une notification de contrôle préalable au titre de l'article 27, paragraphe 2, point a), du règlement (CE) nº 45/2001 (le «règlement») concernant le traitement des données relatives à la santé[1]. Ce traitement a pour objet de garantir le respect des exigences prévues dans le statut des fonctionnaires dans le cadre des visites médicales préalables à l'engagement, des examens médicaux annuels ainsi que des congés de maladie des membres du personnel de l'agence. Les documents reçus par le CEPD sont les suivants:

- un projet de politique concernant le traitement des données relatives à la santé au sein de l'ENISA;
- une déclaration de confidentialité sur la protection des données à caractère personnel relatives à la santé;
- un extrait de la déclaration de confidentialité de l'ENISA mentionnant les articles 10, paragraphe 3 et 7, paragraphe 3; ainsi que

[1] La notification a été envoyée au CEPD le 10 décembre 2011, mais des informations et documents importants faisaient défaut. Un échange de correspondance a eu lieu entre le CEPD et l'ancien délégué à la protection des données. En date du 19 juin 2015, le CEPD a effectué une visite à l'ENISA.

- des extraits de contrats (sur la confidentialité et la protection des données) conclus avec le prestataire médical externe.

Dans la mesure où il s'agit d'une notification ex post, le délai de deux mois pour l'adoption d'un avis par le CEPD ne s'applique pas.

La notification et les documents correspondants sont analysés à la lumière des lignes directrices du CEPD concernant les données relatives à la santé sur le lieu de travail (ci-après les «lignes directrices»)[2]. L'avis conjoint du CEPD concernant le traitement des données relatives à la santé par 18 agences[3] est également applicable en l'espèce.

Le CEPD déterminera les pratiques de l'ENISA qui ne semblent pas conformes aux principes énoncés dans le règlement ou dans les lignes directrices puis adressera à l'ENISA les recommandations appropriées.

1) <u>Traitement de données à caractère personnel pour le compte des responsables du traitement</u>

L'ENISA a conclu un contrat avec un prestataire médical externe, et au titre de ce contrat, un conseiller médical chargé de fournir des services médicaux aux membres du personnel de l'ENISA a été sélectionné.

L'article I.9 du contrat sur la protection des données mentionne les droits des prestataires externes. En effet, l'ENISA est soumise à des obligations quant au traitement des données à caractère personnel du prestataire et ce dernier bénéficie également de droits au titre du règlement. Le contrat a néanmoins pour objet la fourniture de services médicaux aux membres du personnel de l'ENISA. L'ENISA devrait dès lors ajouter un paragraphe sur les **obligations** du prestataire au regard du traitement des données à caractère personnel des membres du personnel de l'agence.

Compte tenu du caractère sensible des opérations de traitement examinées ici, l'ENISA aurait pu prévoir une clause élaborée sur mesure, plutôt que de recourir à une clause classique de protection des données. Bien que le contrat ait malheureusement déjà été signé, le CEPD recommande à l'ENISA de le réviser et d'ajouter une clause relative aux **obligations** du prestataire concernant le traitement des données à caractère personnel des membres du personnel de l'Agence. S'agissant des droits du prestataire découlant du règlement, l'ENISA doit mieux informer ce dernier par l'intermédiaire d'une déclaration de confidentialité ou tout autre moyen jugé opportun.

2) <u>Durée de conservation</u>

La notification indique que les **certificats d'aptitude préalables à l'engagement** sont conservés dans les dossiers personnels pour une durée indéfinie. À la lumière de l'article 4, paragraphe 1, point e), il convient que l'ENISA fixe une durée maximale de conservation, nécessaire à la réalisation des finalités pour lesquelles les certificats d'aptitude sont collectés. Le CEPD recommande que les certificats d'aptitude soient conservés dans les dossiers personnels pendant dix ans après la fin de la période d'activité d'un membre du personnel ou après le dernier versement de la pension de retraite.

[2] Émises en septembre 2009 et publiées sur le site web du CEPD.
[3] Publié le 11 février 2011, il concerne 18 agences, dossier 2010-0071.

En ce concerne les **données médicales liées aux visites médicales préalables à l'engagement**, la notification de l'ENISA devrait indiquer que ces données sont conservées par le service médical de la Commission pour une durée maximale de 30 ans après que le dernier document a été versé au dossier médical.

Concernant les **données médicales conservées par le conseiller médical externe**, la notification indique que celles-ci sont conservées pendant un an, tandis que le projet de politique mentionne une période de 30 ans, conformément aux règles du CEPD. Cette incohérence demande des éclaircissements.

L'ENISA devrait donc indiquer clairement ces délais de conservation dans la notification.

3) <u>Information de la personne concernée</u>

L'ENISA a élaboré un projet de politique complet concernant le traitement des données relatives à la santé publiées sur l'intranet, lequel explique la procédure et les bonnes pratiques en matière de protection des données dans le cadre des visites médicales préalables à l'engagement, des examens médicaux annuels ainsi que des certificats médicaux. Toutefois, au titre de l'article 11 du règlement, les membres du personnel doivent être informés du traitement de leurs données à caractère personnel **avant** que celles-ci ne soient collectées, par souci d'équité et de transparence.

<u>Déclarations de confidentialité sur les visites médicales préalables à l'engagement et les examens médicaux annuels</u>
La déclaration de confidentialité communiquée au CEPD concerne uniquement le traitement des certificats médicaux en cas d'absence. L'ENISA devrait élaborer deux déclarations de confidentialité claires et concises sur les visites médicales préalables à l'engagement et sur les examens médicaux annuels, comprenant toutes les informations prévues aux articles 11 et 12 du règlement.

La déclaration de confidentialité sur les visites médicales préalables à l'engagement devrait être jointe à la lettre envoyée au candidat retenu l'invitant à se soumettre à la visite médicale préalable à l'engagement.

Quant à la déclaration de confidentialité sur les examens médicaux annuels, tous les membres du personnel devraient pouvoir y accéder facilement lorsqu'on leur demande de se soumettre à l'examen médical annuel, que ce soit auprès du conseiller médical externe de l'ENISA ou auprès d'un médecin privé.

<u>Identité du responsable du traitement</u>
Conformément aux articles 11, paragraphe 1, point a), et 12, paragraphe 1, point a), il importe qu'une personne de contact au sein des ressources humaines soit indiquée sur les trois déclarations de confidentialité (y compris celle concernant les certificats médicaux) de sorte que les membres du personnel puissent prendre contact directement avec la personne chargée du dossier, permettant ainsi de formuler des demandes écrites et d'assurer la confidentialité. Le CEPD rappelle qu'en pratique, les ressources humaines de l'ENISA sont responsables de la gestion interne du traitement des opérations examinées ici. Du point de vue juridique, l'ENISA est responsable de ces opérations de traitement.

Droits d'accès et de rectification

Sur la base des articles 11, paragraphe 1, point e), et 12, paragraphe 1, point e), du règlement, l'ENISA devrait expliquer, dans toutes les déclarations de confidentialité, comment les membres du personnel peuvent exercer leurs droits d'accès et de rectification, afin de s'assurer qu'ils comprennent pleinement leurs droits.

Concernant les droits d'accès, l'ENISA devrait préciser que les membres du personnel peuvent avoir un accès indirect - et non un accès direct - à leurs rapports psychiatriques et psychologiques par l'intermédiaire d'un médecin de leur choix[4].

S'agissant du droit de rectification, l'ENISA devrait mentionner que les membres du personnel n'ont pas seulement le droit de corriger les erreurs administratives dans leur dossier médical mais également de le compléter, en ajoutant les avis d'autres médecins afin de garantir l'exhaustivité du dossier.

Délais de conservation des données

À la lumière des articles 11, paragraphe 1, point f), sous ii), et 12, paragraphe 1, point f), sous ii), du règlement, l'ENISA devrait clairement indiquer, dans les déclarations de confidentialité concernées, le délai de conservation des données médicales et des certificats d'aptitude préalables à l'engagement.

L'ENISA devrait adopter l'ensemble des recommandations du CEPD en vue de respecter le règlement et mettre à jour la notification, le cas échéant. Dans le cadre du suivi, le CEPD attend de l'ENISA qu'elle envoie dans un délai de trois mois tous les documents pertinents mis à jour, afin de démontrer qu'elle a mis en œuvre les recommandations précitées.

Veuillez croire, Monsieur, en l'assurance de ma considération distinguée.

(signé)

Wojciech Rafał WIEWIÓROWSKI

Cc: M. Aidan RYAN, chef de l'administration
M^me^ Athena BOURKA, déléguée à la protection des données

[4] À cet égard, l'ENISA devrait renvoyer à la Conclusion 221/04 du Collège des Chefs d'Administration du 19 février 2004.