EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
CONTRÔLEUR ADJOINT

[…]
Délégué à la protection des données
Centre européen de prévention et de contrôle des maladies (ECDC)
Granits väg 8
171 65 Solna
Suède

Bruxelles, le 17 janvier 2018
WW/OL/sn/D(2018)0109 **C 2017-1077**
Veuillez utiliser l'adresse edps@edps.europa.eu pour toute correspondance

Objet: Avis de contrôle préalable concernant l'accès aux locaux de l'ECDC (dossier CEPD 2017-1077)

Madame/Monsieur […],

Le 30 novembre 2017, le Contrôleur européen de la protection des données (ci-après le «CEPD») a reçu une notification de contrôle préalable au titre de l'article 27 du règlement (CE) nº 45/2001[1] (ci-après le «règlement») concernant l'«accès aux locaux».[2]

Après avoir analysé la notification et le dossier joint, le CEPD considère que l'«accès aux locaux» ne relève pas de l'obligation de contrôle préalable. Néanmoins, nous avons quelques remarques et recommandations à formuler au sujet du traitement notifié.

1. Nécessité d'un contrôle préalable

En vertu de l'article 27 du règlement, les traitements «susceptibles de présenter des risques particuliers» sont soumis au contrôle préalable du CEPD. Le paragraphe 2 dudit article énumère les traitements susceptibles de présenter de tels risques.

L'ECDC a notifié l'«accès aux locaux» en vue d'un contrôle préalable au titre de l'article 27, paragraphe 2, point a), dans lequel les «traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté» sont répertoriés comme des traitements à risque.

Les «mesures de sûreté» mentionnées dans cet article ne renvoient pas à des mesures de sécurité relatives à la gestion de l'accès aux locaux ou de sécurité de l'information. Au contraire, le

[1] JO L 8 du 12.1.2001, p. 1.
[2] Étant donné qu'il s'agit d'une notification ex post, le délai de deux mois ne s'applique pas. Ce dossier a été traité dans les meilleurs délais.

CEPD considère que cette expression se réfère à des mesures prises à l'encontre de personnes physiques dans le cadre d'une procédure pénale (ou administrative)[3].

Il s'avère qu'aucun des autres critères justifiant le besoin d'un contrôle préalable en vertu de l'article 27 ne s'applique non plus. En conséquence, l'«accès aux locaux» **n'est pas soumis à un contrôle préalable**.

Cela étant dit, le CEPD a néanmoins plusieurs recommandations à formuler en vue de garantir la conformité de l'«accès aux locaux» avec le règlement. L'analyse ci-dessous ne couvre pas tous les aspects du règlement, mais uniquement ceux qui nécessitent des améliorations ou donnent lieu à des commentaires.

2. Faits et analyse

L'article 4, paragraphe 1, point e), du règlement dispose que 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».

Selon le formulaire de notification, l'ECDC conserve les données à caractère personnel des visiteurs pendant cinq ans après leur visite; pour les permis de longue durée, l'ECDC conserve lesdites données pendant cinq ans après qu'une personne a arrêté de travailler à l'ECDC. La notification n'inclut pas de documents complémentaires montrant les besoins de l'ECDC en matière de sécurité justifiant ce laps de temps.

Bien qu'il revienne en premier lieu à l'ECDC de prévoir un délai de conservation conformément à l'article 4, paragraphe 1, point e), que l'on peut paraphraser comme «aussi longtemps que nécessaire, pendant une durée aussi courte que possible», ce délai de conservation semble excessif.

À titre de comparaison, la Commission européenne conserve les données d'identification pendant six mois après la visite/l'expiration du badge[4]. Une période similaire pourrait être acceptable pour l'ECDC. Pour que le CEPD accepte des délais de conservation plus longs, les institutions de l'Union doivent démontrer leurs besoins et obligations spécifiques, comme en ce qui concerne la sûreté nucléaire[5].

Le CEPD **recommande** de réduire le délai de conservation à une durée proportionnelle.

En vertu de 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 et pour lesquelles elles sont traitées ultérieurement».

Selon les informations fournies, l'ECDC conserve une «copie des pages pertinentes du document [d'identification]» (page 6 de la procédure interne, pour les visiteurs occasionnels) et une «copie de la carte d'identité/du passeport des travailleurs externes» (page 15 de la

[3] Voir également les versions linguistiques française et allemande qui utilisent respectivement «mesures de sûreté» (au lieu de «mesure de sécurité») et «Sicherungsmaßregeln» (au lieu de «Sicherheitsmaßnahmen»).

[4] Contrôle d'accès physique général de la Commission européenne (http://ec.europa.eu/dpo-register/details.htm?id=44001 – dernière mise à jour le 30 mars 2017); l'OLAF suit certaines règles spécifiques (https://ec.europa.eu/dpo-register-olaf/details.htm?id=966 – dernière mise à jour le 26 mai 2016).

[5] Veuillez consulter le document https://edps.europa.eu/sites/edp/files/publication/11-07-15_acs_jrc_en.pdf. pour voir un exemple de ces obligations spécifiques. Pour d'autres affaires précédentes, veuillez consulter les documents https://edps.europa.eu/data-protection/our-work/publications/opinions-non-prior-check/access-control-premises-eda_fr et https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/control-system-iris-scan-european-central_en. Pour une notification récente d'une agence de l'Union avec des besoins élevés en matière de sécurité et un délai de conservation court, veuillez consulter le document https://edps.europa.eu/sites/edp/files/register/notification_file/1440-2017-2045_-_notification.pdf.

procédure interne, pour l'accès des travailleurs externes en dehors des heures de travail). L'ECDC collecte également des informations concernant la date de domiciliation des personnes en Suède ou dans un autre pays de l'Union (page 15 de la procédure interne).

Si le CEPD accepte d'enregistrer des données comme le nom, la date de naissance, le domicile, la nationalité et le numéro du document d'identité, les institutions de l'Union ne devraient pas faire de copie des documents en entier, puisque ce faisant, elles pourraient collecter des informations à caractère personnel non pertinentes. À titre de comparaison, certaines institutions de l'Union utilisent, ou prévoient d'utiliser, des scanners extrayant automatiquement et uniquement les données pertinentes des documents d'identité. D'autres enregistrent seulement les données nécessaires, sans faire de copie du document en entier. La raison pour laquelle l'ECDC collecte des données sur la date de domiciliation des personnes n'est pas claire non plus.

Le CEPD **recommande** à l'ECDC de réévaluer les données dont il a besoin et de ne plus faire de copies des documents d'identité des visiteurs/travailleurs externes et, à la place, de n'enregistrer que les données pertinentes, sur une liste des visiteurs, par exemple.

En vertu de l'article 22 du règlement, les responsables du traitement sont tenus de «[mettre] en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques».

[…][6].

[…]

3. Conclusion

Bien que l'«accès aux locaux» ne soit pas soumis au contrôle préalable au titre de l'article 27 du règlement, les délais de conservation soulèvent des questions relatives à la conformité avec le règlement, ainsi qu'il ressort de l'analyse ci-dessus. Compte tenu du principe de responsabilité, le CEPD attend de l'ECDC qu'il mette en application les recommandations susmentionnées et décide donc de **clôturer le dossier**.

Cordialement,

(signé)

Wojciech Rafał WIEWIÓROWSKI

Cc: […], Chef de la section Services administratifs, ECDC

[6] Concernant la gestion du risque pour la sécurité de l'information en général, voir https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en.