LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Avis sur les notifications en vue d'un contrôle préalable reçues du délégué à la protection des données de l'Agence ferroviaire européenne (AFE) concernant le système de courrier électronique et le système de courrier électronique d'arrière-plan de l'AFE

Bruxelles, le 6 décembre 2012 (dossiers 2012-136 et 137)

1. PROCÉDURE

Le 10 février 2012, le contrôleur européen de la protection des données (le «**CEPD**») a reçu du délégué à la protection des données (le «**DPD**») de l'Agence ferroviaire européenne (l'«**AFE**» ou l'«**Agence**») deux notifications en vue d'un contrôle préalable concernant, respectivement, le système de courrier électronique de l'AFE et le système de courrier électronique d'arrière-plan de l'AFE. Avant de procéder aux notifications, l'AFE a consulté le CEPD quant à la nécessité d'un contrôle préalable conformément à l'article 27, paragraphe 3, du règlement (CE) n° 45/2001 (ci-après le «**règlement**»). Les notifications étaient accompagnées des projets de documents suivants:

- Politique 2.0 Utilisation des ressources propres de l'AFE en matière de TIC [(1)] («**TIC**»)
- Politique 2.1 Gestion des identités et des accès («**IAM**»)
- Politique 2.2 Politique d'utilisation acceptable de l'internet («**politique internet**»)
- Politique 2.3 Politique en matière de communications électroniques («**ECP**»)
- Politique 2.4 Utilisation acceptable du courrier électronique («**politique relative au courrier électronique**»)
- Politique 2.5 Politique relative à la sécurité des informations électroniques («**EISP**»).

L'arrière-plan du système de courrier électronique est la partie qui concerne les communications entre les serveurs de courrier électronique (par exemple Microsoft Exchange) et le monde extérieur/les utilisateurs internes (par opposition à la partie client, qui est le logiciel qu'utilisent les utilisateurs pour accéder à leur courrier électronique, par exemple Microsoft Outlook, un navigateur Internet pour le webmail, etc.). Les deux notifications ne présentant pas de différences nettes, le CEPD les traitera conjointement. Le présent avis désigne conjointement les deux notifications par le terme de «Politique relative au courrier électronique».

Le CEPD a demandé à l'AFE de fournir des informations complémentaires les 2 avril, 2 juillet, 7 et 28 septembre et 26 octobre 2012. Les réponses ont été reçues les 4 mai, 5 et 25 septembre,

[(1)] Technologies de l'information et de la communication.#

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
Email: edps@edps.europa.eu - Site Internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

15 et 17 octobre et 15 novembre 2012. [(2)] Le 10 mai 2012, le CEPD a décidé de prolonger de deux mois le délai imparti pour rendre un avis, conformément à l'article 27, paragraphe 4, du règlement, en raison de la complexité du dossier. Une réunion a été organisée entre le CEPD et les services de l'AFE le 10 octobre 2012 afin de préciser certains points.

2. FAITS

Le présent avis en vue d'un contrôle préalable porte sur la politique de l'AFE relative au système de courrier électronique et au système de courrier électronique d'arrière-plan, telle que décrite dans la Politique relative au courrier électronique et dans l'ECP. Sur le plan organisationnel, le service de l'institution ou de l'organe responsable du traitement est l'unité administrative.

Outre ces notifications spécifiques, l'AFE a adressé au CEPD, à titre de documents de référence, ses politiques écrites concernant les TIC, l'IAM et l'EISP. Bien que ces documents ne relèvent pas de l'objet du présent avis d'un point de vue technique, le CEPD y fera référence pour autant qu'ils soient pertinents.

2.1. Finalités du traitement

Les finalités de la Politique relative au courrier électronique déclarées par l'AFE sont les suivantes:

- définir l'usage approprié et inapproprié du système de courrier électronique;
- s'assurer que les systèmes de courrier électronique de l'Agence sont utilisés à des fins conformes à la mission de l'Agence;
- informer la communauté de l'Agence de l'applicabilité des règles et des politiques de l'AFE s'agissant des courriers électroniques;
- prévenir les interruptions et l'usage abusif des systèmes et des services de courrier électronique.

2.2. Catégories de personnes concernées

Les notifications décrivent les catégories de personnes concernées comme suit:

- toute personne dont l'adresse électronique apparaît dans les champs «À», «De», «Copie» et/ou «Copie cachée» d'un message électronique, dès que ces messages ont été traités par les serveurs de courrier électronique de l'AFE;
- s'agissant de la gestion du carnet d'adresses électroniques, l'ensemble du personnel des institutions, agences et organes européens avec lesquels a été mise en place et signée une convention relative à l'article 7 du règlement n° 45/2001 («Transferts de données»);
- les agents statutaires de l'AFE, les fonctionnaires et les agents statutaires d'autres institutions, agences ou organes européens, les «Experts nationaux détachés», les stagiaires et les sous-traitants;
- les citoyens européens et de pays tiers.

[(2)] Les réponses exhaustives à toutes les questions posées les 2 juillet et 7 septembre 2012 n'ont été reçues que le 17 octobre 2012. Le CEPD a dès lors considéré la période allant du 2 juillet au 17 octobre comme une période de suspension ininterrompue du délai.

2.3. Usage autorisé et interdit

Selon l'AFE, les services de courrier électronique ne doivent pas être utilisés à des fins dont l'on pourrait raisonnablement s'attendre à ce qu'elles causent une pression excessive sur de quelconques ressources de communications électroniques ou fassent obstacle à l'utilisation de ressources électroniques par d'autres personnes. Dans ce contexte, les utilisateurs de courrier électronique doivent s'abstenir en particulier:

- d'envoyer ou de faire suivre des chaînes de lettres ou leurs équivalents dans d'autres services;
- de «spammer», c'est à dire d'utiliser les systèmes de communications électroniques à des fins allant au-delà de leur champ d'application prévu en vue d'amplifier la diffusion massive de messages électroniques non sollicités;
- d'adresser des «lettres piégées», c'est à dire d'envoyer un message extrêmement volumineux ou plusieurs messages électroniques à un ou plusieurs destinataires et, donc, de compromettre l'utilisation par les destinataires des systèmes et des services de communications électroniques;
- de mettre en œuvre volontairement d'autres pratiques telles que les «attaques par déni de service» qui entravent la disponibilité des services de communications électroniques.

L'usage personnel accessoire est autorisé pour autant qu'il (i) n'entrave pas l'exploitation par l'Agence de ses ressources de communications électroniques, (ii) ne nuise pas à la mission professionnelle de l'utilisateur ou à ses autres obligations envers l'Agence, ou (iii) ne fasse pas supporter à l'Agence des coûts supplémentaires importants.

2.4. Contrôle de l'usage

La Politique relative au courrier électronique précise que les courriers indésirables et les virus sont automatiquement filtrés avant d'atteindre les utilisateurs. En outre, la politique relative aux TIC informe les utilisateurs que l'Agence contrôlera régulièrement les modes d'utilisation des ressources en TIC et indique que cette mesure vise à assurer le bon fonctionnement des systèmes d'information de l'AFE et à éviter les atteintes à la sécurité. La politique relative aux TIC indique également que le contenu des communications ne fera l'objet d'aucun contrôle.

Les utilisateurs de courrier électronique de l'AFE ne doivent pas utiliser les services de courrier électronique pour transférer par l'internet certaines données comme des noms d'utilisateur, des mots de passe, des numéros de sécurité sociale et des numéros de compte. Les utilisateurs ne doivent pas utiliser le système de courrier électronique pour transférer des données sensibles, sauf dans le respect des politiques de l'AFE en matière de protection des données.

2.5 Accès aux messages électroniques sans le consentement de l'utilisateur

La partie IV du document décrit les règles relatives aux demandes d'examen du courrier électronique sans le consentement de l'utilisateur. Le document indique que, de manière générale, l'AFE n'a pas besoin du consentement d'une personne pour examiner les fichiers stockés sur son ordinateur car ces fichiers ne répondent pas à la définition d'«enregistrement de communication électronique» énoncée dans l'ECP. Cependant, lorsqu'ils examinent ce type de fichiers, les collègues sont soumis à une obligation de respect des communications personnelles. Tout examen doit être limité au minimum nécessaire.

Pour accéder au courrier électronique du titulaire d'un poste, l'AFE considère qu'il est nécessaire de demander le consentement du titulaire du compte dans le respect des règles

énoncées dans la partie V de l'ECP. L'accès sans consentement ne peut être demandé que dans des «*circonstances très limitées*», comme décrites dans l'ECP et dans la Politique relative au courrier électronique (partie IV B):

- L'agent ne travaille plus à l'AFE ou est décédé. Dans ce cas, l'accès est autorisé dans des conditions normales sans soumission de demande officielle d'accès sans consentement.
- Agent en congés. Le chef d'unité/de secteur ou le supérieur hiérarchique direct (le «demandeur») doit demander à l'avance à un agent l'autorisation d'accéder, si nécessaire, à son courrier électronique pendant la période de congés afin d'assurer la continuité des activités. Cette autorisation peut également être demandée à l'agent alors qu'il est en congés. Si cela s'avère impossible, le demandeur doit suivre les procédures énoncées par l'ECP pour obtenir un accès sans consentement.
- Enquêtes pénales ou dossiers sensibles: cette hypothèse vise les situations suivantes: (i) l'agent ne peut pas ou ne veut pas accorder son consentement, (ii) l'agent ne doit pas être alerté, (iii) une enquête pénale est en cours concernant un ancien titulaire de poste. Dans un tel cas, le demandeur doit entrer en relation avec le responsable de la sécurité de l'AFE qui suivra les procédures prévues pour obtenir un accès sans consentement.

Si certaines personnes souhaitent obtenir un accès sans le consentement de la personne, elles doivent compléter un formulaire spécifique intitulé «Formulaire d'accès sans consentement» (sauf dans les cas relevant du premier point ci-dessus).

La procédure à suivre pour obtenir un accès sans consentement est décrite de manière plus détaillée dans l'ECP. L'accès aux communications électroniques doit être autorisé par le directeur exécutif ou par le chef de l'administration, ou par toute autre fonction déléguée, en consultation avec le délégué à la protection des données et le responsable de la sécurité informatique de l'AFE. L'AFE doit toujours demander l'avis du DPD de l'AFE et/ou des services juridiques de l'AFE avant d'accéder sans consentement à des enregistrements de communications électroniques (voir l'ECP, p. 14 de la version anglaise).

L'autorisation sera limitée à la consultation du contenu la plus restreinte et aux mesures les plus restreintes nécessaires pour résoudre la situation. En cas d'urgence, l'ECP permet un accès immédiat sans autorisation et avec les garanties appropriées. L'autorisation doit être demandée sans délai.

2.6. Catégories de données à caractère personnel

Les catégories de données concernées sont:

- pour les messages électroniques, l'en-tête (informations concernant le trafic)/l'objet du message, le corps du message (c'est-à-dire son contenu) et les pièces jointes;
- pour le carnet d'adresses: le nom, le prénom, l'alias (informations de connexion), le numéro de téléphone professionnel, l'unité ou le secteur, l'adresse électronique.

2.7. Transferts de données/destinataires

S'agissant des courriers électroniques, les destinataires sont potentiellement toutes les personnes dans le monde disposant d'une adresse électronique, y compris les membres du personnel des institutions, agences et organes de l'UE. S'agissant du carnet d'adresses, les destinataires comprennent le personnel de l'AFE, les services de courrier électronique des

institutions de l'UE et le personnel des agences et organes de l'UE avec lesquels l'AFE a conclu un accord bilatéral.

2.8. Conservation des données

Les données personnelles figurant dans les courriers électroniques sont conservées aussi longtemps que la personne concernée dispose d'un compte de messagerie électronique actif et pendant un délai de 90 jours après la désactivation de ce compte ou de 13 mois après sa suppression des fichiers journaux et des supports de sauvegarde. Les données personnelles figurant dans les carnets d'adresses sont conservées aussi longtemps que la personne concernée est employée au sein de l'AFE.

2.9. Droits des personnes concernées

Les personnes concernées seront informées par l'intermédiaire d'une Note à l'attention du personnel «Utilisation des ressources propres de l'AFE en matière de TIC», de la politique relative aux TIC, de l'IAM, de l'ECP et de la Politique relative au courrier électronique.

Lorsqu'un agent entre en fonctions, il est informé du règlement qui protège, en particulier, le droit d'accès aux données et de rectification de celles-ci dont disposent les personnes concernées et le droit dont elles disposent de demander à l'AFE de rectifier sans délai toute donnée inexacte ou incomplète ou de supprimer les données lorsque leur traitement est illicite. Les personnes concernées peuvent exercer leurs droits en contactant l'AFE par courrier électronique. L'AFE doit traiter les demandes de rectification dans un délai d'un mois à compter de l'introduction de la demande. Il doit être répondu aux demandes de verrouillage et de suppression dans un délai de trois mois. Les personnes concernées peuvent s'adresser au DPD à tout moment par courrier électronique.

2.10. Mesures de sécurité

Plusieurs mesures de sécurité spécifiques au système sont mises en œuvre et décrites dans la Politique relative au courrier électronique:

- le système est intégré dans le système d'IAM mis en place au sein de l'Agence. Les utilisateurs sont informés du fait qu'ils ne doivent pas communiquer leur mot de passe, y compris au service d'assistance;
- afin de lutter contre les virus, certains types de pièces jointes peuvent être supprimés au niveau de la passerelle de courrier électronique de l'Agence. Le cas échéant, les destinataires en sont avertis par courrier électronique. Les pièces jointes étant susceptibles de contenir des virus et d'autres logiciels malveillants, les utilisateurs sont informés qu'ils doivent ouvrir uniquement les pièces jointes provenant d'une source digne de confiance et faire suivre les éléments suspects au service d'assistance;
- les courriers indésirables sont automatiquement filtrés au niveau de la passerelle de l'Agence. Les courriers électroniques identifiés de façon évidente comme des courriers indésirables sont supprimés sur la base d'une liste noire de domaine avant qu'ils n'atteignent la passerelle de courrier électronique. Les courriers électroniques suspects sont classés dans le dossier «Courrier indésirable» local;
- l'accès aux fichiers journaux est réservé aux administrateurs du système de courrier électronique (opérations quotidiennes) et aux autres autorités compétentes (par exemple l'OLAF).

L'EISP décrit des mesures supplémentaires couvrant tous les systèmes, au nombre desquelles:

- la nécessité de gérer les risques et de définir des contrôles rentables sur le plan économique afin de se prémunir contre ces risques;
- une description des fonctions et des responsabilités couvrant également les aspects de sécurité;
- les règles applicables aux informations classées;
- une liste concernant la procédure de sécurité nécessaire qui doit être définie;
- des contrôles opérationnels et techniques (sauvegardes, processus de gestion des correctifs et des modifications...);
- la nécessité de dispenser une formation et de sensibiliser les personnes à la sécurité.

3. Aspects juridiques

3.1. Contrôle préalable

Le présent avis en vue d'un contrôle préalable concerne les politiques de l'AFE se rapportant à l'usage du courrier électronique, y compris les traitements de données visant à contrôler le comportement des utilisateurs. Le présent avis évalue donc la mesure dans laquelle les traitements de données décrits ci-dessus, effectués par les intervenants pertinents au sein de l'AFE, sont conformes au règlement.

3.1.1. Applicabilité du règlement

Le règlement (CE) n° 45/2001 s'applique au «*traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*» et au traitement «*effectué par toutes les institutions et organes communautaires dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire*». Pour les motifs énoncés ci-dessous, tous les éléments rendant le règlement applicable sont réunis en l'espèce.

Premièrement, le contrôle de l'usage du courrier électronique suppose la collecte et le traitement ultérieur de *données à caractère personnel*, telles qu'elles sont définies à l'article 2, point a), du règlement (CE) n° 45/2001. Ce contrôle inclut des enregistrements du trafic des courriers électroniques indiquant de manière détaillée l'usage que fait chaque membre du personnel de l'AFE du courrier électronique (données transactionnelles) ainsi que le contenu des messages électroniques.

Deuxièmement, comme le précisent les notifications, les données à caractère personnel collectées font l'objet d'un «*traitement automatisé*», tel que défini à l'article 2, point b), du règlement, et d'un traitement manuel. En effet, les informations personnelles sont d'abord collectées de manière automatisée (enregistrement automatique des fichiers journaux) et gérées de manière automatisée par le système (filtrage des courriers indésirables et des virus) et peuvent ensuite être analysées par les membres du personnel informatique compétents.

Enfin, le traitement est effectué par une institution de l'UE, en l'espèce l'Agence ferroviaire européenne, dans le cadre du droit de l'UE (article 3, paragraphe 1, du règlement). Par conséquent, tous les éléments rendant le règlement applicable sont réunis en l'espèce.

3.1.2. Motifs justifiant le contrôle préalable

L'article 27, paragraphe 1, du règlement soumet au contrôle préalable du 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 établit une liste des traitements susceptibles de présenter de tels risques. Cette liste comprend, au point a), «*les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions...*» et, au point b), «*les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement*».

Étant donné, d'une part, que le contrôle de l'usage du courrier électronique tel que décrit dans les politiques soumises peut conduire à l'évaluation du comportement des utilisateurs (afin de déterminer si leur usage est conforme ou non à la Politique relative au courrier électronique de l'AFE) et, d'autre part, que ce contrôle peut impliquer la collecte de données relatives à des suspicions (en cas de suspicion de comportement illicite) et d'autres types de données sensibles, ce contrôle et les traitements de données s'y rapportant doivent être soumis à un contrôle préalable conformément à l'article 27, points a) et b), du règlement.

Le contrôle préalable conformément à l'article 27 du règlement doit intervenir, en principe, avant le début du traitement. Le CEPD regrette donc profondément, en l'espèce, que les notifications ne lui aient pas été soumises avant le début des opérations de traitement.

3.1.3. Notification et date à laquelle le CEPD rendra son avis

Les notifications ont été reçues le 10 février 2012. Le délai dans lequel le CEPD doit rendre son avis conformément à l'article 27, paragraphe 4, du règlement a été suspendu pendant 178 jours en vue de l'obtention d'informations complémentaires.

Par ailleurs, le 10 mai 2012, le CEPD a prolongé le délai de deux mois supplémentaires en raison de la complexité et de la sensibilité des questions en jeu et de la préparation en parallèle par le CEPD de lignes directrices horizontales sur la surveillance électronique.

L'avis doit donc être rendu au plus tard le 6 décembre 2012.

3.2. Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que s'il trouve son fondement juridique dans les dispositions de l'article 5 du règlement. Les notifications justifient les opérations de traitement sur le fondement de l'article 5, point a), du règlement, à savoir un traitement nécessaire à l'exécution d'une mission effectuée dans l'intérêt public. En outre, la Politique relative au courrier électronique fait référence dans diverses situations au consentement de la personne concernée (article 5, point d), du règlement). Cette base juridique sera analysée de manière plus détaillée ci-après (points 3.2.1. et 3.2.2.).

Enfin, le CEPD se concentrera sur certains traitements spécifiques décrits dans l'ECP et dans la Politique relative au courrier électronique qui suscitent des inquiétudes spécifiques en matière de licéité (points 3.2.3. à 3.2.6.).

3.2.1. Article 5, point a) - traitement nécessaire à l'exécution d'une mission effectuée dans l'intérêt public

L'article 5, point a), du règlement prévoit que le traitement de données peut être effectué s'il «*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*».

Pour déterminer si le traitement est conforme à l'article 5, point a), du règlement, deux éléments doivent être pris en compte: il convient de déterminer, premièrement, si le traité ou d'autres actes juridiques prévoient une mission effectuée dans l'intérêt public sur la base de laquelle le traitement est effectué (*base juridique*) et, deuxièmement, si les opérations de traitement sont effectivement nécessaires à l'exécution de cette mission, c'est-à-dire à la réalisation des objectifs visés (*nécessité*).

- Base juridique

Le CEPD relève en premier lieu que le règlement comporte plusieurs dispositions qui sont pertinentes pour apprécier la licéité du contrôle de l'usage du courrier électronique par l'AFE. En particulier, le règlement indique à son considérant 30 qu'«*[i]l peut être nécessaire de contrôler les réseaux d'ordinateurs fonctionnant sous la responsabilité des institutions et organes communautaires en vue de prévenir un usage non autorisé*». Comme souligné ci-dessus, l'un des objectifs poursuivis par l'AFE lorsqu'elle procède à un contrôle du courrier électronique est de prévenir tout usage de cet instrument en violation de la loi ou des politiques internes de l'AFE ou de quelque autre manière non autorisée.

En outre, l'article 37, paragraphe 2, du règlement prévoit une base juridique supplémentaire qui autorise l'AFE à réaliser un traitement de données très spécifique, à savoir la conservation de données relatives au trafic, en l'espèce les fichiers journaux. L'article 37, paragraphe 2, prévoit en particulier que les données relatives au trafic peuvent être traitées aux fins de la gestion du budget des télécommunications et du trafic, y compris la vérification de l'usage autorisé des systèmes de télécommunication. La notion de «*vérification de l'usage autorisé*» est essentielle car elle concerne l'éventuel usage des données relatives au trafic au-delà de la gestion du budget et du trafic. En particulier, elle permet d'utiliser les données relatives au trafic pour assurer la sécurité du système et des données ainsi que le respect du statut du personnel ou d'autres dispositions telles que celles énoncées dans la Politique relative au courrier électronique.

En outre, le CEPD considère que l'AFE, en sa qualité d'employeur, assume certains devoirs et est liée par certaines obligations découlant du droit du travail qui peuvent être considérés comme des fondements juridiques justifiant un traitement proportionné. Par exemple, le devoir de l'AFE de se protéger de toute responsabilité liée à des actions de travailleurs peut également justifier le traitement. Ceci peut inclure le traitement de catégories particulières de données, dans certaines circonstances (voir le point 3.3.).

Enfin, les politiques publiées par l'AFE constituent un autre élément utile pour déterminer l'existence ou non d'une base juridique appropriée aux fins de l'article 5, point a), du règlement, en ce qu'elles établissent des règles relatives au contrôle des ressources électroniques en vue, notamment, d'assurer la sécurité et la vérification de l'usage autorisé.

- Nécessité

Comme décrit ci-dessus, l'un des principaux objectifs du traitement examiné est de s'assurer que les systèmes de courrier électronique de l'Agence sont utilisés à des fins conformes à la mission de l'Agence, comme exposé dans la Politique relative au courrier électronique, et de prévenir les interruptions et l'usage abusif des systèmes et des services de courrier électronique. Le CEPD relève que l'AFE estime nécessaire de procéder à un contrôle de l'usage de ses systèmes de courrier électronique en vue d'être en mesure de prévenir ou de détecter des violations de la Politique relative au courrier électronique ou des atteintes à la

sécurité. Par conséquent, il apparaît qu'un contrôle sélectif et licite des systèmes de courrier électronique peut être considéré comme nécessaire, au moins dans une certaine mesure, pour exécuter la tâche consistant à assurer un usage conforme à la Politique relative au courrier électronique et, par conséquent, pour assurer la sécurité générale des ressources en TIC de l'AFE.

L'AFE estime également nécessaire de mettre en place un certain contrôle pour être en mesure d'exercer, le cas échéant, ses droits et obligations découlant du droit du travail. Par exemple, l'AFE déclare que, si elle n'était pas en mesure de contrôler la façon dont une personne soupçonnée d'adopter une conduite contraire à sa politique (par exemple, en divulguant des documents confidentiels) utilise le courrier électronique, elle pourrait ne pas disposer des éléments de preuve nécessaires pour engager une procédure disciplinaire.

À la lumière de ce qui précède, le CEPD relève que le traitement notifié peut être considéré comme nécessaire pour atteindre les objectifs visés par la politique. Les exigences en matière de conformité à l'article 5, point a), du règlement semblent donc satisfaites en principe. Lorsqu'elle contrôle l'usage du courrier électronique, l'AFE doit toujours respecter les obligations de nécessité et de proportionnalité conformément au principe de la qualité des données, comme abordé au point 3.4.

3.2.2. Article 5, point d) - consentement de la personne concernée

L'ECP indique qu'en principe l'AFE n'examine les données de communications électroniques qu'avec le consentement de l'utilisateur. Pour être valable, le consentement doit être libre, spécifique et informé. L'utilisateur doit être informé des opérations de traitement, en particulier de celles fondées sur son consentement, ainsi que de certains éléments fondamentaux concernant ces opérations, y compris les conséquences de ses décisions.

L'utilisation du consentement fait l'objet de limitations spécifiques dans les cas où la personne concernée se trouve dans une situation de dépendance ou de faiblesse vis-à-vis du responsable du traitement. Tel est le cas en particulier en ce qui concerne les relations de travail. [(3)] Le CEPD considère que le consentement ne peut être utilisé comme un fondement valable pour le traitement de données de communications électroniques personnelles dans le cadre d'une relation professionnelle que dans des cas limités et exceptionnels.

3.2.2.1. Accès aux courriers électroniques en l'absence de l'utilisateur

Il existe un cas dans lequel il pourrait exceptionnellement être fait usage du consentement pour accéder à des communications électroniques, il s'agit du cas dans lequel l'accès vise à permettre la continuité des activités, c'est-à-dire lorsque l'utilisateur est absent ou ne travaille plus et que l'employeur a besoin d'accéder aux courriers électroniques professionnels. [(4)] Bien que, comme indiqué, le consentement ne constitue pas la condition préalable idéale pour un tel traitement de données personnelles, l'«accord» de la personne concernée contribue à réduire les tensions sur le lieu de travail.

Dans un tel cas, l'utilisateur doit se voir communiquer toutes les informations nécessaires, notamment concernant les raisons motivant la demande d'accès, l'urgence de l'affaire, la nature et la portée des informations recherchées et les autres informations visées à l'article 11

[(3)] Voir, par exemple, l'avis du groupe de travail «article 29» sur la définition du consentement, 13 juillet 2011 (WP187), p. 13 et suiv.
[(4)] Voir l'avis du 18 janvier 2010 - «Procédure de la Cour des comptes d'accès au disque/courrier électronique privé» (dossier 2009-0620).

du règlement. L'AFE a soumis au CEPD un formulaire de consentement à utiliser dans ces cas. Le formulaire comporte des champs concernant (i) les raisons motivant l'octroi de l'accès, (ii) l'étendue de l'accès, (iii) la période d'accès, et (iv) les obligations de proportionnalité et de confidentialité qui doivent être respectées. Le CEPD formule les observations suivantes concernant le contenu du formulaire:

- le formulaire doit indiquer de manière claire et visible que le consentement est libre et révocable à tout moment et que l'utilisateur ne subira aucune conséquence négative s'il refuse d'accorder son consentement;
- l'expression «tous les documents nécessaires à la conduite des activités de l'Agence» est trop large. Le CEPD recommande de remplacer cette formule par une définition plus précise;
- il est nécessaire d'inclure les informations suivantes, prévues à l'article 11: l'identité du responsable du traitement, les destinataires ou les catégories de destinataires des données, l'existence d'un droit d'accès à tout courrier électronique reçu et expédié par l'intermédiaire du compte pendant la période considérée.

L'article 5, point a), ne doit être pris comme base juridique que lorsqu'il est impossible d'obtenir le consentement de l'utilisateur (si ce dernier est injoignable ou n'est pas en mesure de donner son consentement) ou de mettre en place d'autres solutions organisationnelles ou techniques (par exemple des boîtes aux lettres fonctionnelles, voir ci-après). Le CEPD est d'avis que l'accès aux données, dans le cadre de la procédure, ne pourrait être considéré comme nécessaire pour atteindre les objectifs poursuivis par l'AFE que si celle-ci peut prouver que le membre du personnel a reçu des informations claires et complètes sur l'usage du disque privé et de la messagerie électronique professionnelle et privée, que l'urgence de l'accès demandé peut être démontrée et que le consentement de l'utilisateur n'a pas pu être obtenu. Ces différents critères de nécessité devront être démontrés au cas par cas. En outre, chaque fois qu'il est accédé aux données en l'absence de l'utilisateur, celui-ci doit en être informé individuellement.

Il convient également de souligner qu'une telle procédure d'accès ne doit pas être comprise comme s'inscrivant dans une procédure d'enquête administrative à l'encontre d'un membre du personnel. Plus précisément, cette procédure ne peut servir à contourner les règles fixées pour les procédures d'enquête administrative ou les procédures disciplinaires à l'encontre d'un membre du personnel. Le DPD de l'AFE doit démontrer, dans son avis écrit, qu'il a analysé cet aspect.

En complément ou en alternative à la méthodologie ci-dessus, l'AFE peut envisager de créer des boîtes aux lettres communes et de demander aux destinataires d'y copier les correspondances professionnelles. Dans ce cas, l'accès aux boîtes aux lettres communes peut être accordé en principe à tous les membres de l'unité. Cette approche réduirait considérablement la nécessité d'accéder aux courriers électroniques individuels à des fins de continuité des activités.

En ce qui concerne les comptes de messagerie électronique d'utilisateurs ne travaillant plus à l'Agence, les membres du personnel devraient être invités, avant leur départ, à supprimer de leur compte de messagerie électronique tous les contenus privés. Afin de traiter de manière proactive les demandes d'accès formulées par d'anciens membres du personnel, le CEPD estime qu'il serait opportun de fournir une copie des courriers électroniques privés, qui ont été désignés comme tels par l'utilisateur, (ou du disque privé comportant ces courriers électroniques) sur un CD/DVD.

Il conviendrait de modifier/revoir la partie IV B de la Politique relative au courrier électronique (telle que décrite au point 2.5. ci-dessus) et les parties correspondantes de l'ECP en vue de se conformer aux recommandations ci-dessus.

3.2.2.2. Accès aux fichiers stockés sur l'ordinateur d'une personne

La Politique relative au courrier électronique indique que «*l'examen de fichiers stockés sur l'ordinateur d'une personne ne nécessite généralement pas que cette personne ait donné son consentement à l'accès car ces fichiers ne répondent pas à la définition d'"enregistrement de communication électronique" énoncée dans l'ECP*». Le CEPD n'est pas d'accord avec cette déclaration car l'«enregistrement de communication électronique» est défini par l'ECP comme «*le contenu des communications électroniques créées, envoyées, transférées, auxquelles il est répondu, transmises, distribuées, diffusées,* ***stockées, conservées, copiées, téléchargées,*** *affichées, vues, lues ou imprimées par un ou plusieurs systèmes ou services de communications électroniques*» (gras ajouté). Dès lors, les fichiers stockés dans l'ordinateur d'un utilisateur peuvent tout à fait contenir des données personnelles, y compris des courriers électroniques. Le CEPD considère que les fichiers stockés dans les ordinateurs de personnes doivent être soumis aux mêmes règles que celles concernant l'accès aux courriers électroniques en l'absence d'un utilisateur.

Le CEPD recommande par conséquent à l'AFE d'appliquer à ce type d'accès les mêmes règles que celles prévues pour l'accès au courrier électronique d'un utilisateur en l'absence de celui-ci (voir le point 3.2.2.1. ci-dessus).

3.2.3. Comptes webmail personnels

La Politique relative au courrier électronique indique qu'«*elle s'applique à l'usage par tout titulaire de poste de comptes de messagerie électronique personnels par le biais d'un navigateur, comme indiqué ci-dessous*». Au cours d'échanges ultérieurs avec le CEPD, l'AFE a précisé que «*tout titulaire d'un poste au sein de l'AFE utilisant l'infrastructure de TIC de l'AFE peut utiliser un compte de messagerie électronique privé. Bien que ce compte de messagerie ne fasse pas partie du système informatique de l'AFE, il sera indiqué, lors de son usage par l'intermédiaire d'une connexion Internet, que l'accès s'effectue par les adresses IP de l'Agence. À cet égard, il est attendu des utilisateurs qu'ils adoptent un comportement conforme aux dispositions de la politique*».

De manière générale, l'employeur ne peut réglementer ni exercer d'influence sur l'usage que font les employés de leurs comptes webmail personnels, même si l'accès à ces comptes s'effectue au moyen des connexions de l'Agence. Les comptes webmail personnels ne relèvent généralement pas de la portée de la sphère d'influence du contrôleur; ils appartiennent à la sphère privée et par conséquent l'employeur, en principe, n'a pas le droit d'intervenir. Le fait que l'accès à un compte personnel au travail apparaisse comme ayant été effectué au moyen des adresses IP de l'Agence ne semble pas constituer un motif valable permettant de soumettre les comptes webmail personnels à la Politique relative au courrier électronique de l'AFE. Ceci est également démontré par la parfaite incompatibilité avec certaines des dispositions de l'Agence, telles que celles concernant l'activation et la désactivation du compte de messagerie électronique, les restrictions, l'usage personnel accessoire, l'accès sans consentement, etc.

Il pourrait exister certaines exceptions à cette règle générale, comme l'interdiction de télécharger des fichiers ou même d'accéder à des comptes de messagerie personnels, pour autant qu'elles soient justifiées et proportionnées. Cependant, la Politique relative au courrier électronique ne fournit aucune information concernant les situations spécifiques dans lesquelles

elle s'appliquerait à l'usage des comptes webmail personnels. L'application générale de cette politique aux comptes webmail personnels ne peut être maintenue.

Sur des fondements similaires, le CEPD estime que la disposition de l'ECP selon laquelle «*il est interdit aux titulaires de postes de l'AFE de rechercher, d'utiliser ou de divulguer des informations personnelles dans des communications électroniques sans autorisation*» est trop intrusive et restrictive. Cette disposition a une portée trop étendue. Elle implique que les utilisateurs de l'AFE ne sont pas autorisés à utiliser les courriers électroniques à des fins personnelles ou pour transmettre des messages professionnels comportant des données personnelles. La première lecture serait en contradiction avec le fait que l'ECP autorise l'usage personnel accessoire, tandis que la seconde semblerait irréaliste.

Le CEPD invite donc l'AFE à réexaminer les dispositions ci-dessus et à reformuler les parties correspondantes de la Politique relative au courrier électronique afin de tenir compte des considérations émises ci-dessus.

3.2.4. Accès aux documents publics

L'ECP comporte une définition spécifique de l'expression «enregistrement de communication électronique de l'Agence» («ECR»). La définition est la suivante:

«*[l]es enregistrements de communications électroniques se rapportant à l'activité administrative de l'Agence sont considérés comme des documents publics,* ***que l'Agence soit ou non propriétaire des systèmes de ressources de communications électroniques ou des appareils utilisés*** *pour créer, envoyer, transférer, répondre à, transmettre, stocker, conserver, copier, télécharger, afficher, consulter, lire ou imprimer ces documents ou les enregistrer de quelque autre manière.* ***Les autres enregistrements, bien qu'ils n'appartiennent pas à l'Agence****, peuvent néanmoins être divulgués en qualité d'enregistrements publics en vertu de la législation de l'UE s'ils se rapportent à l'activité de l'Agence*» (gras ajouté).

La définition ci-dessus des ECR de l'Agence présente des liens évidents avec la notion de document public aux fins du règlement n° 1049/2001 relatif à l'accès du public aux documents. Le fait que les ECR de l'Agence soient considérés comme des enregistrements publics peut en effet impliquer l'obligation de donner accès à ces documents en vertu du règlement précité. Toutefois, la définition fournie semble aller au-delà de la définition de l'UE du «document public». À cet égard, le CEPD souligne que le règlement n° 1049/2001 exige, pour s'appliquer, que les documents soient des documents «*détenus par une institution*», c'est-à-dire «*établis ou reçus par elle et en sa possession, dans tous les domaines d'activité de l'Union européenne*». Le CEPD invite par conséquent l'AFE à réfléchir à cette définition afin de s'assurer de sa conformité avec le règlement précité.

L'ECP indique également qu'«*aux fins de la présente politique, tous les enregistrements de communications électroniques stockés sur les équipements de communication, vidéo, audio et informatiques appartenant à l'Agence ou contrôlés par celle-ci seront réputés être des enregistrements de communication électronique de l'Agence. Cela inclurait les communications électroniques personnelles*» (soulignement ajouté). Si le sens de la dernière phrase n'est pas tout à fait clair, le CEPD se doit de souligner l'éventuelle incohérence du passage précité découlant de l'idée selon laquelle les communications électroniques personnelles pourraient faire l'objet d'une divulgation publique. Tant qu'elles sont vraiment personnelles (non liées à l'exécution des tâches de l'Agence), les communications personnelles ne relèvent pas du champ d'application du règlement n° 1049/2001. Le CEPD recommande donc à l'AFE de réexaminer et/ou de préciser le passage en cause.

3.2.6. Interception de conversations téléphoniques

L'ECP prévoit que «*les conversations téléphoniques audio ou vidéo ne doivent pas être enregistrées ou contrôlées sans que les participants en aient été avisés, sauf en cas d'approbation expresse d'un tel enregistrement ou contrôle par un tribunal*».

À la lumière de la jurisprudence de la Cour européenne des droits de l'homme, le CEPD considère que l'interception de communications électroniques ne peut intervenir qu'en présence d'une base juridique suffisamment précise et spécifique. [(5)] En particulier, l'interception doit être clairement autorisée par la loi, fondée sur un instrument juridique spécifique définissant les circonstances et les conditions dans lesquelles elle peut être réalisée et offrir des garanties appropriées contre les risques d'abus. Un acte administratif ne peut en général être considéré comme suffisant à cet égard.

Le CEPD n'a connaissance d'aucun instrument juridique autorisant, au sens indiqué ci-dessus, l'interception de communications électroniques par l'AFE. Les bases juridiques générales pour les enquêtes administratives et les procédures disciplinaires ne sont habituellement pas considérées comme une base juridique suffisante pour les interceptions téléphoniques. Bien au contraire, conformément au considérant 19 du règlement, l'AFE devrait ***s'adresser*** aux autorités compétentes dans les États membres lorsqu'elle estime que des interceptions de communications doivent être réalisées sur ses réseaux de télécommunications, conformément aux dispositions nationales applicables, mais elle n'est pas habilitée à réaliser les interceptions elle-même.

Le CEPD estime par conséquent que l'AFE ne dispose pas d'une base juridique suffisamment précise et spécifique pour réaliser des interceptions de communications électroniques sur le lieu de travail. Il recommande à l'AFE de supprimer le passage précité de l'ECP.

3.3. Traitement portant sur des catégories particulières de données

Le contrôle de l'usage du courrier électronique peut révéler des catégories particulières de données à caractère personnel. Le règlement définit ces données comme étant les données à caractère personnel «*qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle*» (article 10). En particulier, le contenu de certains courriers électroniques peut révéler des détails très intimes de la vie personnelle d'un individu, comme les préférences sexuelles, des données sur la santé ou les orientations politiques. Même le traitement de données relatives au trafic, comme les fichiers journaux de courriers électroniques, peut parfois être considéré comme une catégorie particulière de données, par exemple dans le cas où les courriers électroniques sont adressés à des «destinataires sensibles» comme un syndicat, un parti politique et des organisations similaires.

Le traitement de catégories particulières de données est en principe interdit, sauf en cas d'application de l'une des exceptions prévues à l'article 10 du règlement. L'article 10, paragraphe 2, point b), du règlement dispose que l'interdiction ne s'applique pas lorsque le traitement est «*nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités*». Un certain contrôle de l'usage du courrier électronique peut être estimé

[(5)] Voir, par exemple, CEDH, *Kruslin c. France* (11801/85), arrêt du 24 avril 1990, point 33; CEDH, *Malone*, précité, point 68.

nécessaire pour que l'AFE puisse assurer la sécurité du système et des données ainsi que le respect du statut du personnel ou d'autres dispositions.

Ceci inclurait par exemple le droit de l'AFE d'interdire la consultation ou l'échange de contenus ou d'informations à caractère sexuel sur le lieu de travail. Le contrôle des informations sensibles peut également se justifier dans certains cas pour permettre à l'employeur d'exercer ses droits en tant qu'employeur, comme le droit d'engager des procédures disciplinaires en vue, notamment, du licenciement d'employés se livrant à des activités illicites, telles que la consultation et le téléchargement de matériels promouvant des actes criminels. Par conséquent, le CEPD considère qu'en sa qualité d'employeur l'AFE a des droits et obligations en matière de droit du travail qui peuvent justifier un traitement nécessaire et proportionné de données sensibles d'utilisateurs dans le cadre d'enquêtes internes.

En ce qui concerne le traitement de données à caractère personnel dans le cadre d'enquêtes administratives, le CEPD renvoie l'AFE aux lignes directrices relatives aux enquêtes administratives et aux procédures disciplinaires. (6)

3.4. Qualité des données

3.4.1. Adéquation, pertinence et proportionnalité

Conformément à l'article 4, paragraphe 1, point c), du règlement (CE) n° 45/2001, 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. C'est ce que l'on appelle le principe de la qualité des données.

L'objectif déclaré de la Politique relative au courrier électronique de l'AFE est le suivant:

- définir l'usage approprié et inapproprié du système de courrier électronique;
- s'assurer que les systèmes de courrier électronique de l'Agence sont utilisés à des fins conformes à la mission de l'Agence;
- informer la communauté de l'Agence de l'applicabilité des règles et des politiques de l'AFE en ce qui concerne les courriers électroniques;
- prévenir les interruptions et l'usage abusif des systèmes et des services de courrier électronique.

Comme décrit ci-dessus, le traitement des courriers électroniques à des fins de sécurité consiste essentiellement en l'inspection automatisée systématique des courriers électroniques acheminés par le réseau de télécommunications d'une institution en vue d'éliminer les virus, les autres logiciels malveillants et les courriers indésirables. Ce processus est mis en œuvre par des moyens automatisés et, par conséquent, n'implique normalement aucun traitement manuel des données à caractère personnel. Le CEPD n'a pas d'observation particulière à formuler sur cette approche, qui correspond à la pratique courante dans ce type de situations.

Ceci étant, le CEPD souligne que l'examen individuel de données de communications électroniques liées au courrier électronique, y compris le contenu de celui-ci, ne peut intervenir qu'en présence d'une suspicion suffisante d'actes répréhensibles corroborée par des preuves initiales concrètes et dans le cadre d'une enquête administrative. L'accès doit être proportionné et ne pas aller au-delà de ce qui est approprié et proportionné eu égard aux circonstances

[6] Lignes directrices relatives au traitement de données à caractère personnel dans le cadre d'enquêtes administratives et de procédures disciplinaires entamées par les institutions et organes de l'Union européenne, 23 avril 2010, disponibles sur le site Internet du CEPD.

particulières. Une procédure claire fondée sur une approche progressive et proportionnée devrait être mise en place à cet égard. En ce qui concerne le traitement de données à caractère personnel dans le cadre d'enquêtes administratives, le CEPD renvoie l'AFE aux lignes directrices relatives aux enquêtes administratives et aux procédures disciplinaires. [7]

L'ECP fait référence aux circonstances suivantes dans lesquelles l'accès sans consentement est autorisé: 1) lorsque l'accès est nécessaire et conforme à la loi; 2) lorsqu'il existe des raisons valables de croire que des violations de la loi ou de la politique de l'Agence ont été commises; 3) lorsqu'il existe des «circonstances impérieuses» telles que définies dans l'annexe; 4) dans des «circonstances opérationnelles critiques sensibles au facteur temps» telles que définies dans l'annexe. Elle précise en outre que, sauf dans les «cas d'urgence», ces mesures doivent être autorisées à l'avance et par écrit par le directeur exécutif ou le chef de l'administration, ou par toute autre personne exerçant une fonction déléguée, en consultation avec le délégué à la protection des données de l'AFE et le responsable de la sécurité informatique de l'AFE.

Le CEPD se félicite du fait que le DPD soit consulté avant tout accès à une messagerie électronique sans consentement. Toutefois, il tient à souligner que des expressions comme «circonstances impérieuses», «circonstances opérationnelles critiques sensibles au facteur temps» et «cas d'urgence», bien qu'elles soient définies, sont trop générales et se chevauchent. Il recommande par conséquent à l'AFE de réexaminer l'utilisation de ces termes dans ses politiques. En particulier, l'AFE devrait préciser et clarifier davantage ces définitions.

3.4.2. Loyauté et licéité

L'article 4, paragraphe 1, point a), du règlement exige que les données soient traitées loyalement et licitement. La question de la licéité a été analysée ci-dessus (voir le point 3.2.). La question de la loyauté est étroitement liée au type d'informations fournies aux personnes concernées, ce qui sera étudié au point 3.8.

3.4.3. Exactitude

Conformément à l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel doivent être «*exactes et, si nécessaire, mises à jour*» et «*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*». L'AFE doit prendre toutes les mesures raisonnables pour s'assurer que les données sont à jour et pertinentes. À cet égard, voir également le point 3.8.

3.5. Conservation des données

L'article 4, paragraphe 1, point e), du règlement prévoit 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 les notifications et la Politique relative au courrier électronique, les données sont conservées aussi longtemps que la personne concernée dispose d'un compte de messagerie électronique actif et pendant un délai de 90 jours après la désactivation de ce compte et de 13 mois après sa suppression des fichiers journaux et des supports de sauvegarde.

[7] Précitées.

Ce calendrier n'est pas tout à fait conforme à l'article 37 du règlement, qui prévoit des mesures spécifiques s'agissant de la conservation des données relatives au trafic et à la facturation. L'article 37, paragraphe 2, du règlement prévoit en effet que les données relatives au trafic doivent être effacées ou rendues anonymes dès que possible, et en tout état de cause au plus tard six mois après leur collecte, à moins que leur conservation ultérieure soit nécessaire à la constatation, à l'exercice ou à la défense d'un droit dans le cadre d'une action en justice en instance devant un tribunal. L'AFE peut donc décider de conserver les journaux pendant une durée maximale de 6 mois.

Si le contrôle des fichiers journaux ou des données relatives au trafic conduit l'AFE à soupçonner qu'une personne a enfreint la Politique relative au courrier électronique, l'AFE sera autorisée à conserver les fichiers journaux suspects en vue de «*la constatation, [de] l'exercice ou [de] la défense d'un droit dans le cadre d'une action en justice en instance devant un tribunal*». Dans ce contexte, l'article 20 du règlement est également pertinent en ce qu'il prévoit des limitations possibles au principe d'effacement immédiat des données visé à l'article 37, paragraphe 1, notamment lorsque la limitation constitue une mesure nécessaire pour «*assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales*». Le CEPD a interprété cette disposition comme couvrant non seulement les enquêtes pénales, mais également les procédures disciplinaires. [(8)]

Par conséquent, si nécessaire, les fichiers journaux peuvent être traités dans le cadre d'une enquête administrative, qu'il s'agisse d'une infraction pénale ou disciplinaire. Il convient de noter que cette mesure ne doit être prise qu'au cas par cas, lorsque l'on peut légitimement soupçonner qu'une personne a commis une infraction à la Politique relative au courrier électronique, ou au statut du personnel, ou qu'elle a commis une infraction pénale, et que l'AFE a ouvert une enquête administrative. À la fin des six premiers mois, il doit être procédé à une évaluation afin de déterminer si les données collectées et les vérifications effectuées sont raisonnablement de nature à justifier la poursuite de l'enquête (qui devrait être officiellement ouverte) ou le lancement d'une procédure disciplinaire. Ce n'est que lorsque le résultat de cette évaluation est positif que les données de trafic peuvent être conservées plus de six mois; il convient de noter que dans ces cas, seules les parties pertinentes des fichiers journaux doivent être conservées.

3.6. Transferts de données

Les articles 7, 8 et 9 du règlement énumèrent une série d'obligations qui s'appliquent lorsque les responsables du traitement transfèrent des données à caractère personnel à des tiers. Les règles diffèrent selon que le transfert est destiné i) à des institutions ou organes de l'UE (conformément à l'article 7), ii) à des destinataires relevant de la directive n° 95/46 (conformément à l'article 8) ou iii) à d'autres types de destinataires (conformément à l'article 9).

Selon les notifications, seuls peuvent accéder aux données, en interne, le responsable de la sécurité informatique et le directeur informatique. Au cours d'autres échanges avec le CEPD, l'AFE a ajouté les destinataires internes suivants, en précisant que les données à caractère personnel pourraient leur être transférées dans le cadre de la «Procédure de gestion des incidents» (incidents techniques, incidents de sécurité), c'est-à-dire dès lors que survient un incident suffisamment grave pour qu'il en soit référé à ce niveau de la hiérarchie:

- Directeur exécutif,

[(8)] Voir, par exemple, l'avis du CEPD du 22 décembre 2005 - Enquêtes administratives internes de la Banque centrale européenne (2005-0290).

- Délégué à la protection des données,
- Chef de l'unité administrative,
- Chef d'unité concerné,
- Chef de secteur concerné,
- Chef du secteur des ressources humaines,
- Chef du secteur de la gestion financière des TI,
- Responsable de la sécurité des TIC,
- Administrateur du système informatique,
- Prestataires de services informatiques.

Le CEPD souligne que l'article 7 du règlement prévoit que les données à caractère personnel doivent être transférées pour «*l'exécution légitime de missions relevant de la compétence du destinataire*». Pour se conformer à cette disposition, lors du transfert de données à caractère personnel, l'AFE doit s'assurer *(i)* que le destinataire possède les compétences adéquates et *(ii)* que le transfert est nécessaire. Le responsable du traitement doit évaluer la nécessité du transfert (et des données à transférer) au cas par cas.

En l'espèce, il apparaît que la responsabilité de la gestion interne du contrôle de l'usage du courrier électronique incombe au chef de la gestion financière des TI, à l'administrateur du système et au responsable de la sécurité des TIC. Le chef de l'administration a, d'autre part, la qualité de responsable des opérations de traitement liées à des enquêtes administratives et à des mesures disciplinaires. Le CEPD recommande à l'AFE de revoir la liste des destinataires à la lumière de ce qui précède et d'évaluer au cas par cas si les transferts effectués par le responsable de la sécurité des TIC, l'administrateur du système ou le chef de la gestion financière des TI à ces destinataires sont conformes à l'article 7. En effet, seules les personnes auxquelles incombe la responsabilité de décider du lancement d'une enquête administrative et de la gestion du système semblent compétentes à la lumière de l'article 7.

En outre, dans des circonstances particulières, les données peuvent être communiquées à titre temporaire aux catégories suivantes de destinataires au sein des institutions et organes de l'Union européenne:

- l'OLAF et/ou l'OIDC dans le cadre de leurs enquêtes,
- le Médiateur, à sa demande,
- le contrôleur européen de la protection des données, à sa demande,
- les juges de la Cour de justice de l'Union européenne, à leur demande.

Le CEPD considère que les transferts d'informations à l'OLAF, à l'OIDC, à la Cour de justice de l'Union européenne, au Médiateur et/ou au CEPD aux fins de l'accomplissement de leurs missions officielles sont en principe conformes à l'article 7. L'AFE doit cependant en évaluer la nécessité au cas par cas.

Les notifications mentionnent également des transferts de données au bureau du procureur. Les transferts de données au bureau du procureur seront traités dans le cadre de l'avis en vue d'un contrôle préalable concernant l'enquête administrative et les procédures disciplinaires. En effet, ce type de transfert n'interviendra que s'il ressort de l'enquête administrative qu'un membre du personnel pourrait avoir commis une infraction pénale.

Selon les notifications, il n'est prévu aucun transfert vers des pays tiers ou des organisations internationales.

3.7. Droits d'accès et de rectification, verrouillage et effacement

L'article 13 du règlement dispose que la personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, du responsable du traitement, la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données.

Le CEPD rappelle que le droit d'accès est obligatoire, sauf exception, et que l'AFE doit mettre en place les procédures autorisant son exercice. Le droit d'accès comprend, notamment, le droit d'être informé et d'obtenir une copie des données traitées concernant une personne sous une forme intelligible. L'AFE doit mettre en place les procédures appropriées afin de garantir que les utilisateurs pourront exercer leur droit d'accès. Le CEPD prend bonne note du fait que les personnes concernées peuvent exercer leurs droits en envoyant un courrier électronique à une boîte aux lettres fonctionnelle et que l'AFE s'efforce de répondre à leur demande dans un délai d'un mois.

Dans certains cas, le responsable du traitement des données peut être en mesure d'invoquer l'une des exceptions visées à l'article 20, paragraphe 1, du règlement pour reporter l'octroi des droits d'accès ou de rectification. En l'espèce, ce report peut être licite, entre autres, lorsqu'une telle limitation constitue une mesure nécessaire pour «*a) assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales*». Lorsqu'elle décide d'invoquer une exception, l'AFE doit procéder à une évaluation au cas par cas des circonstances du traitement de données spécifique considéré.

Lorsque l'AFE invoque une exception pour reporter l'octroi de l'accès, elle doit tenir compte du fait que les limitations d'un droit fondamental ne peuvent s'appliquer de manière systématique. L'AFE doit, dans chaque cas, déterminer si les conditions d'application de l'une des exceptions sont réunies. En outre, comme le prévoit l'article 20 du règlement, la mesure doit être «nécessaire». Ce «critère de nécessité» doit donc être appliqué au cas par cas. Lorsque l'AFE applique une exception, elle doit se conformer à l'article 20, paragraphe 3, selon lequel «*la personne concernée est informée conformément au droit communautaire des principales raisons qui motivent cette limitation et de son droit de saisir le contrôleur européen de la protection des données*». Cependant, l'AFE peut se prévaloir de l'article 20, paragraphe 5, pour reporter l'information conformément à la disposition suivante: *«L'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1.».*

Conformément à l'article 14 du règlement, la personne concernée a le droit de rectifier les données inexactes ou incomplètes. Étant donné la nature des données (fichiers journaux reliés à des identifiants d'utilisateurs et à des adresses IP) et la manière dont elles sont collectées (consignation automatique), la possibilité de rectification des données paraît improbable. Cependant, en principe, l'AFE doit reconnaître l'existence de ce droit, qui peut s'appliquer dans un nombre limité de cas, par exemple lorsqu'une personne utilise l'identifiant d'un autre utilisateur. La boîte aux lettres fonctionnelle peut également être utilisée aux fins des demandes de suppression et de rectification et une réponse doit être fournie, selon les notifications, dans un délai de 3 mois civils.

Le CEPD attire l'attention de l'AFE sur les droits d'effacement et de verrouillage en application des articles 16 et 15 du règlement. La personne concernée a le droit d'obtenir l'effacement des données si leur traitement est illicite. Conformément à l'article 15, la personne concernée a le droit d'obtenir du responsable du traitement le verrouillage des données lorsque

leur exactitude est contestée, pendant un délai permettant au responsable du traitement de vérifier l'exactitude des données; lorsqu'elles ne sont plus utiles au responsable du traitement mais qu'elles doivent être conservées à titre probatoire, ou lorsque leur traitement est illicite et que la personne concernée s'oppose à leur effacement et exige à la place leur verrouillage.

3.8. Information de la personne concernée

Conformément aux articles 11 et 12 du règlement, les personnes qui collectent des données à caractère personnel sont tenues d'informer les personnes concernées que des données les concernant sont collectées et traitées. Les personnes concernées ont également le droit d'être informées, entre autres choses, des finalités du traitement, des destinataires des données et des droits spécifiques qui leur sont accordés en cette qualité de personnes concernées.

Afin d'assurer la conformité avec les articles 11 et 12, l'AFE a pris (ou va prendre) les mesures suivantes:

- Les utilisateurs des TIC seront officiellement informés de la procédure de contrôle par l'intermédiaire d'une Note à l'attention du personnel «Utilisation des ressources propres de l'AFE en matière de TIC».
- En outre, dans un délai de 30 jours à compter de l'entrée en vigueur de la politique relative aux TIC, tous les utilisateurs actuels devront signer le «formulaire de reconnaissance [de la politique en matière de TIC] de l'AFE» (le «formulaire»). Les nouveaux utilisateurs devront signer le même formulaire avant de se voir accorder un accès aux ressources TIC de l'AFE. Le formulaire comporte une confirmation que l'utilisateur a lu, compris et accepté la politique relative aux TIC.
- L'ensemble des politiques est disponible sur le site intranet du service Gestion financière des TI dans la rubrique PROJETS de politiques - Consultation AFE.
- Le responsable de la sécurité informatique organisera dans les mois à venir un programme spécifique de sensibilisation, dans le cadre du Programme de sécurité en matière d'informations électroniques.

3.8.1. Les voies de communication des informations

Le CEPD souligne la nécessité pour l'AFE de s'assurer que la voie choisie pour communiquer des informations relatives aux le contrôle permette aux personnes concernées de prendre effectivement connaissance de son contenu. Le CEPD estime nécessaire de tenir compte des deux aspects suivants.

Premièrement, pour être effectivement informés, les utilisateurs doivent être directement informés du traitement réalisé concernant leurs données personnelles. La plupart des informations figurant dans les politiques, leur publication sur l'intranet ne semble pas suffisante puisque tous les utilisateurs n'iront pas les vérifier spontanément. Aussi longtemps que cette mesure n'aura pas été prise, le CPDE demande donc instamment à l'AFE d'adresser à chaque membre du personnel une notification individuelle, par exemple un courrier électronique, comportant un lien vers la Déclaration de confidentialité et vers le document relatif à la politique pertinente.

Deuxièmement, les documents pertinents fournissent les informations pertinentes de manière très dispersée; en effet, pour accéder aux informations légalement obligatoires, l'utilisateur doit lire au moins six documents distincts: la Note à l'attention du personnel, la Déclaration de confidentialité, la Politique Internet; la politique d'IAM, la politique relative aux TIC, la politique relative au courrier électronique et l'ECP. Dans certains cas, la relation entre les

différents documents peut ne pas être évidente.

Le CEPD estime qu'il aurait été préférable de communiquer les informations pertinentes, y compris le contenu des articles 11 et 12 du règlement (CE) n° 45/2001, dans un document unique (plutôt que dans des documents distincts). Ceci peut avoir une incidence du point de vue des principes d'équité et de transparence. Afin d'éviter toute confusion et de rendre les politiques plus intelligibles, le CPDE suggère de réunir toutes les informations relatives au contrôle du courrier électronique dans un document unique comportant toutes les informations nécessaires (voir le point suivant 3.8.2.). Ce document pourrait être associé à une Déclaration de confidentialité.

3.8.2. Le contenu de la politique

Le principal objectif des politiques relatives aux TIC est d'informer les utilisateurs de l'usage autorisé et interdit des TIC, d'illustrer le type de contrôle réalisé concernant l'usage et de souligner les conséquences d'un mauvais usage ou d'un usage abusif. S'agissant de la Politique internet de l'AFE, le CEPD tient à formuler les observations suivantes:

- La politique relative aux TIC comme celle relative au courrier électronique indiquent que les TIC de l'AFE doivent être utilisées à des fins professionnelles et que seul un usage personnel limité est autorisé, dans la mesure où il n'empiète pas sur les intérêts de l'AFE. La notion d'«usage personnel limité» n'est pas davantage précisée.
- Les finalités de la réalisation d'un contrôle du courrier électronique ne semblent pas toujours clairement définies. En particulier, la Politique indique clairement qu'il peut être procédé au contrôle des enregistrements du journal en vue d'assurer la fonctionnalité et la sécurité des systèmes, mais ne semble pas claire au sujet de la vérification de l'usage autorisé/des finalités des enquêtes. Dans la mesure où le contrôle vise également à vérifier l'usage autorisé, ce point doit être mentionné de manière explicite.

S'agissant de la Déclaration de confidentialité, le CEPD relève que ce document ne comporte pas toutes les informations nécessaires aux fins des articles 11 et 12. En particulier, les informations concernant i) la finalité du traitement, ii) les destinataires, iii) les catégories de données et iv) l'existence du droit d'accès ne sont pas suffisantes. Le document ne comporte pas non plus les informations complémentaires qui pourraient être considérées comme nécessaires, compte tenu des circonstances particulières, pour assurer un traitement loyal (par exemple la base juridique, la durée de conservation, le droit de saisir le CEPD, etc.).

Le CEPD invite par conséquent l'AFE à remédier à ces lacunes afin de mettre la Déclaration de confidentialité en conformité avec les exigences de l'article 12 du règlement.

3.9. Mesures de sécurité

Conformément aux articles 22 et 23 du règlement, le responsable du traitement et le sous-traitant mettent 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. Ces mesures de sécurité doivent notamment empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération ainsi que toute autre forme de traitement illicite.

L'AFE a confirmé avoir adopté les mesures de sécurité requises par l'article 22 du règlement. Ces mesures sont détaillées dans l'EISP. Le CEPD n'a pas lieu de penser que ces mesures

techniques et organisationnelles ne permettent pas de garantir un niveau de sécurité conforme aux risques que représentent le traitement et la nature des données à caractère personnel à protéger.

Toutefois, le CEPD considère que, dans la mesure où les journaux de courrier électronique sont utilisés non seulement pour de strictes raisons de sécurité mais également pour l'évaluation du comportement, les mesures de sécurité pourraient devoir être renforcées. Le CEPD recommande en particulier l'adoption des mesures suivantes:

1. examiner régulièrement les évaluations des risques décrites dans l'EISP (cet examen pourrait intervenir dans le cadre du plan de sécurité des informations décrit dans cette même politique);
2. s'assurer de la protection des journaux de courrier électronique contre tout accès, modification ou suppression non autorisé, y compris de la part du responsable de la sécurité des TIC et des administrateurs du système informatique;
3. s'assurer de la possibilité, pour chacun des accès aux fichiers journaux de courrier électronique, de remonter jusqu'à une personne physique déterminée;
4. s'assurer que tous les accès aux fichiers journaux de courrier électronique sont justifiés et suivent une procédure bien établie;
5. s'assurer que les responsabilités concernant la gestion des incidents de sécurité, les demandes et les enquêtes internes sont clairement attribuées à des personnes assurant des fonctions spécifiques et suivent des procédures bien établies.

3. CONCLUSION

Le traitement notifié ne peut être mis en œuvre que s'il est pleinement tenu compte des recommandations énoncées dans le présent avis. Pour assurer la conformité au règlement, le CEPD recommande à l'AFE de:

- limiter l'utilisation du consentement à l'accès au courrier électronique des utilisateurs à des fins de continuité des activités sur le fondement des modalités et des conditions décrites au point 3.2.2.1.;
- appliquer à l'accès aux fichiers stockés dans les ordinateurs individuels les mêmes règles que celles prévues pour l'accès au courrier électronique d'un utilisateur en l'absence de celui-ci, comme indiqué au point 3.2.2.2.;
- modifier la partie de la Politique relative au courrier électronique dans la mesure où elle prévoie l'applicabilité de cette dernière aux comptes webmail personnels (point 3.2.3.);
- modifier la disposition de l'ECP en vertu de laquelle «*il est interdit aux titulaires de postes de l'AFE de rechercher, d'utiliser ou de divulguer des informations personnelles dans des communications électroniques sans autorisation*» (point 3.2.3.);
- revoir la définition de l'expression «enregistrement de communication électronique de l'Agence» en vue de la mettre en conformité avec la notion de document public couverte par le règlement n° 1049/2001 relatif à l'accès public aux documents;
- supprimer ou préciser la disposition de l'ECP en vertu de laquelle les enregistrements de communication électronique de l'Agence peuvent inclure des communications électroniques personnelles (point 3.2.4.);
- supprimer la disposition de l'ECP relative à l'interception de communications électroniques;
- mettre en place des mesures de protection techniques et procédurales afin de garantir que le traitement de catégories particulières de données dans le cadre de l'inspection ou du contrôle du courrier électronique soit réduit au minimum et n'intervienne que dans les cas où il est vraiment inévitable;
- ne procéder à l'examen individuel de données de communications électroniques

concernant le courrier électronique, y compris son contenu, qu'en cas de suspicion suffisante d'actes répréhensibles corroborée par des preuves initiales concrètes et dans le cadre d'une enquête administrative. Un tel contrôle ne peut être mis en place qu'une fois que des moyens disponibles moins intrusifs auront été envisagés ou testés. Une procédure claire fondée sur une approche progressive et proportionnée devrait être mise en place à cet égard;

- concernant l'accès sans consentement, préciser et délimiter davantage les expressions telles que «circonstances impérieuses», «circonstances opérationnelles critiques sensibles au facteur temps» et «cas d'urgence»;
- ne conserver les données relatives au trafic des courriers électroniques (y compris les fichiers journaux) que pendant une durée maximale de six mois à compter de leur collecte, conformément à l'article 37, paragraphe 2, du règlement, sauf s'il est nécessaire de les conserver pendant une période plus longue en vue de la constatation, de l'exercice ou de la défense d'un droit dans le cadre d'une action en justice en instance devant un tribunal;
- s'assurer de la conformité des transferts de données aux articles 7 et 8 du règlement, au moyen d'une évaluation concrète de leur caractère nécessaire;
- envisager de réunir toutes les informations concernant le traitement de données relatives à l'usage du courrier électronique dans un document unique comportant toutes les informations nécessaires;
- intégrer et/ou préciser la Politique relative au courrier électronique et la Déclaration de confidentialité conformément aux recommandations formulées au point 3.8.2.;
- examiner régulièrement l'analyse effectuée pour définir les contrôles nécessaires qui doivent être mis en œuvre afin de réduire les risques à un niveau acceptable par la direction;
- renforcer les mesures de sécurité concernant les fichiers journaux de courrier électronique en assurant la traçabilité des opérations de traitement et la limitation de l'accès aux seuls cas de stricte nécessité;
- définir clairement toutes les responsabilités qui permettent d'accéder aux données à caractère personnel des membres du personnel.

Fait à Bruxelles, le 6 décembre 2012.

(**signé**)
Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données