LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis sur la notification de contrôle préalable reçue du délégué à la protection des données de l'Agence ferroviaire européenne (ERA) à propos de l'utilisation du système internet de l'ERA.

Bruxelles, le 6 décembre 2012 (Dossier 2012-0135)

1. PROCÉDURE

Le 10 février 2012, le contrôleur européen de la protection des données («**CEPD**») a reçu du délégué à la protection des données («**DPD**») de l'Agence ferroviaire européenne («**ERA**» ou «l'**Agence**») une notification de contrôle préalable à propos du système internet de l'ERA. Avant le dépôt de la notification, l'ERA a consulté le CEPD quant à la nécessité d'un contrôle préalable au titre de l'article 27, paragraphe 3, du règlement CE 45/2001 (ci-après le «**règlement**»). La notification était accompagnée des projets de documents suivants:

- Politique 2.0 Utilisation des ressources appartenant à l'ERA 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 de la messagerie électronique («**politique relative à la messagerie électronique**»)
- Politique 2.5 Politique relative à la sécurité des informations électroniques («**EISP**»).

Le CEPD a demandé à l'ERA de lui fournir des informations complémentaires les 2 avril, 2 juillet, 7 et 28 septembre, ainsi que les 17, 23 et 26 octobre 2012. Les réponses ont été reçues les 4 mai, 5 et 25 septembre, 15, 17, 18 et 24 octobre ainsi que le 15 novembre 2012.[2] Le 10 mai 2012, le CEPD a décidé en vertu de l'article 27, paragraphe 4, du règlement de proroger de deux mois le délai qui lui est imparti afin de rendre son avis compte tenu de la complexité du dossier. Une réunion a eu lieu entre le CEPD et l'ERA le 10 octobre 2012 afin de clarifier plus avant certaines questions en suspens. Le 15 novembre 2012, le projet d'avis a été envoyé au DPD afin de lui permettre d'apporter ses commentaires. Le CEPD a reçu une réponse le 4 décembre 2012.

[1] Technologie de l'information et de la communication.

[2] Les réponses complètes à toutes les questions posées les 2 juillet et 7 septembre 2012 n'ont été reçues que le 17 octobre 2012. Le CEPD a donc estimé que la période du 2 juillet au 17 octobre constituait une période de suspension continue.

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

2. FAITS

Le présent avis relatif au contrôle préalable concerne la politique internet de l'ERA, telle que décrite dans la politique internet et l'ECP. D'après l'ERA, le service de l'institution ou de l'organe chargé du traitement est l'unité «Administration».

Outre cette notification spécifique, l'ERA a transmis au CEPD comme documents de référence ses politiques écrites relatives aux TIC, à l'IAM et à l'EISP. Bien que ces documents ne tombent pas techniquement dans le champ d'application du présent avis, le CEDP s'y référera si pertinent.

2.1. Finalités du traitement

Selon l'ERA, la politique internet a pour objet:

- d'exposer ce qui constitue une utilisation appropriée ou inappropriée des services internet de l'Agence;
- de veiller à ce que l'utilisation des systèmes et des services internet de l'Agence s'inscrive dans des finalités qui correspondent à la mission de l'Agence;
- d'informer la communauté de l'Agence de l'applicabilité de règles et des politiques de l'ERA lorsqu'elle accède à des services et systèmes internet;
- d'éviter les perturbations et les utilisations abusives de l'infrastructure de l'ERA.

Utilisation appropriée et utilisation inappropriée de l'internet

La section IV de la politique internet («Utilisation acceptable») expose ce qui, selon l'ERA, doit être considéré comme une utilisation appropriée ou une utilisation inappropriée. D'après ce document, toute utilisation impropre de l'internet pourrait compromettre le statut juridique de l'Agence et ne saurait être tolérée. Le document définit en outre une «utilisation inappropriée» comme correspondant notamment aux cas de figure suivants:

a. l'internet ne doit pas être utilisé à des fins illégales ou illicites en cas d'accès via l'infrastructure de l'ERA.[3]
b. l'internet ne doit pas être utilisé d'une façon qui constitue une infraction aux ordonnances administratives, règles ou politiques de l'ERA ou de manière incompatible avec la mission de l'Agence.
c. les personnes doivent limiter leur usage personnel de l'infrastructure de l'ERA en termes d'accès à l'internet. L'ERA permet un usage personnel limité dans le cadre de communications avec la famille et les amis, de l'apprentissage autonome et du service public. L'ERA interdit le recours aux pourriels de masse, l'accès aux installations de réseau et ressources de l'ERA par des personnes non employées par l'agence, les activités commerciales concurrentes et la diffusion de lettres dans le cadre d'une chaîne de lettres.
d. il est interdit aux personnes de consulter, copier, modifier ou détruire des données, logiciels, documentations ou communications de données appartenant à l'ERA ou à un autre membre du personnel sans leur permission.
e. les utilisateurs ne doivent pas envoyer de pièces jointes à un courrier électronique qui sont de taille démesurée.

La section V de la politique internet expose des règles supplémentaires relatives à la sécurité internet. Elle stipule notamment ce qui suit:

a. il est interdit de communiquer des informations relatives aux mots de passe ou comptes;

[3] Y compris, sans pour autant s'y limiter, la violation du droit d'auteur, les obscénités, la calomnie, la fraude, la diffamation, le plagiat, le harcèlement, l'intimidation, la falsification, l'usurpation d'identité, les jeux clandestins, le démarchage dans le cadre de systèmes pyramidaux et les interventions informatiques non autorisées (par ex. au moyen de virus).

b. il est interdit de télécharger des logiciels;
c. si un nouveau programme ou une mise à jour d'un logiciel existant semble être nécessaire, vérifier que tel est le cas auprès du service d'assistance TIC.

Contrôle de l'utilisation

La TIC indique que l'Agence doit régulièrement surveiller les profils d'utilisation des ressources TIC afin de veiller à la fonctionnalité des informations et systèmes d'information de l'ERA et éviter les infractions à la sécurité. Le contenu des communications ne sera en aucun cas surveillé. Toute dérogation aux règles doit être justifiée du fait des besoins du service et être explicitement autorisée par le responsable de l'ITFM[4] et/ou le responsable de la sécurité des TIC, après consultation du comité de direction informatique.

Tout le trafic internet entrant et sortant est automatiquement traité par un ou plusieurs outils de sécurité afin de détecter les virus, programmes malveillants ou logiciels espion. Tout le trafic internet entrant provenant de l'extérieur de l'Agence sera automatiquement analysé par un logiciel anti-virus. En cas de détection de problème, une désinfection sera automatiquement effectuée.[5]

L'Agence utilisera des logiciels de filtrage et autres techniques afin de lutter contre l'accès aux informations inappropriées. En cas d'accès refusé, l'utilisateur recevra un message clair et personnel indiquant les raisons du refus. Les tentatives d'accès seront alors consignées dans les journaux aux fins précitées. L'ERA a affirmé que les journaux n'étaient pas utilisés pour surveiller les comportements individuels, exception faite des cas de figure cités à l'article 20 du règlement relatif à la protection des données. L'ERA a fourni en annexe à la police une liste des catégories filtrées.

D'après la politique internet, l'ERA est habilitée à surveiller toute activité internet entreprise sur son matériel ou ses comptes. L'Agence tient des journaux du trafic internet afin de veiller à la fonctionnalité des systèmes de l'ERA et d'éviter les infractions à la sécurité. Parmi les fichiers journaux, citons notamment:

- le journal des accès aux URL: nom du serveur de l'ERA traitant la demande, date et heure, adresse IP du client, adresse IP du serveur, domaine, chemin d'accès, catégorie, protocole, nombre de visites, le nombre de Mo reçus. L'adresse IP du client est générée dynamiquement;
- le journal des URL bloquées: date et heure, catégorie, règle, type d'analyse, IOOID, URL, protocole;
- le journal de filtrage des URL: date et heure, catégorie, règle, type d'analyse, action de filtrage, URL, protocole.[6]

Il convient de noter que l'ERA ne garde pas les journaux du service d'affectation des adresses IP (journaux DHCP).

2.2. Catégories de personnes concernées

Les catégories de personnes concernées sont les suivantes:

- le personnel de l'ERA,
- les contractants de l'ERA,
- les personnes collaborant avec l'ERA sur le plan professionnel, et

[4] Gestion informatique et des installations.
[5] Politique internet, p. 10-11.
[6] Ibid., p. 11.

- toute personne accédant à de quelconques services internet via l'infrastructure mise à disposition par l'Agence.

2.3. Catégories de données à caractère personnel

Selon la notification, les catégories de données concernées sont les suivantes (à savoir les champs de données enregistrés par le système):

- nom du serveur de l'ERA traitant la demande,
- adresse IP,
- horodatage du traitement des demandes (réception, affectation, modification, résolution, etc.),
- informations relatives au service demandé/consulté,
- toute information que la personne concernée fournit dans le cadre de la transaction.

2.4. Destinataires/transferts de données

La notification indique que les destinataires sont le responsable de la sécurité des TIC et le responsable de l'ITFM.

Lors des échanges ultérieurs avec le CEPD, le contrôleur a ajouté les destinataires internes suivants:

- le directeur exécutif,
- le délégué à la protection des données,
- le responsable de l'unité «Administration»,
- le chef d'unité concerné,
- le chef de secteur concerné,
- le responsable du secteur des Ressources Humaines,
- l'administrateur des services informatiques,
- les prestataires de services informatiques.

En cas de circonstances particulières, des données peuvent être divulguées de façon temporaire:

- aux juges du Tribunal de la fonction publique, à leur demande, ou
- au Parquet, à sa demande, ou
- à l'OLAF et/ou l'IDOC, dans le cadre de leurs enquêtes, ou
- à l'Ombudsman, à sa demande, ou
- au contrôleur européen de la protection des données, à sa demande.

La notification mentionne également les transferts de données au Parquet.

2.5. Conservation des données

Les fichiers journaux (et autres données concernées) sont traités et conservés pendant une durée maximale de 90 jours.

2.6. Droits des personnes concernées

La notification stipule que les personnes concernées ont été informées au moyen d'une note au personnel intitulée «Utilisation des ressources appartenant à l'ERA en matière de TIC», des TIC et de la politique internet.

Les personnes concernées peuvent exercer leur droit d'accès et de rectification en envoyant un message électronique à une boîte aux lettres fonctionnelle en précisant le droit qu'elles

souhaitent exercer. La demande sera traitée par le responsable du traitement des données dans un délai d'un ou de trois mois, selon qu'il s'agit d'une demande concernant l'accès ou le blocage/l'effacement.

2.7. Mesures de sécurité

Plusieurs mesures de sécurité spécifiques du système sont mises en œuvre et décrites dans la politique internet:

- le système est intégré au sein du système d'IAM mis en œuvre par l'Agence. Les utilisateurs sont informés de ne pas communiquer leur mot de passe, même au Service d'assistance;
- afin de lutter contre les virus, le trafic entrant émanant d'en dehors du réseau de l'ERA est automatiquement analysé afin de détecter et d'éliminer les virus, programmes malveillants et logiciels espion;
- l'ERA utilise des logiciels de filtrage afin de lutter contre l'accès aux informations inappropriées (telles que les contenus obscènes, racistes ou faisant l'éloge du terrorisme, etc.);
- l'accès aux fichiers journaux est réservé aux administrateurs des systèmes TIC de l'ERA et au responsable de la sécurité informatique de l'ERA.

Des mesures supplémentaires couvrant tous les systèmes sont décrites dans l'EISP. Elles comprennent notamment:

- la nécessité de gérer les risques et de définir des mesures rentable permettant de se prémunir contre ces risques;
- une description des rôles et responsabilités couvrant également les aspects sécuritaires;
- des règles relatives aux informations classifiées;
- une liste de la procédure de sécurité nécessaire qui doit être définie;
- des mesures opérationnelles et techniques (sauvegardes, correctifs et processus de gestion du changement...);
- la nécessité de former les employés et de les sensibiliser aux aspects sécuritaires.

3. LES ASPECTS LEGAUX

3.1. Contrôle préalable

Le présent avis de contrôle préalable porte sur les politiques de l'ERA relatives à l'utilisation de l'internet au sein de l'Agence, y compris les opérations de traitement des données visant à surveiller le comportement des utilisateurs. Ce faisant, l'avis étudie dans quelle mesure les opérations de traitement des données décrites ci-dessus menées par les intervenants concernés de l'ERA sont conformes au règlement.

3.1.1. Applicabilité du règlement

Le règlement 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 de données à caractère personnel par toutes les institutions et tous les 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-après, toutes les conditions d'application du règlement sont réunies.

Premièrement, le contrôle de l'utilisation de l'internet implique la collecte et le traitement ultérieur de *données à caractère personnel* telles que définies à l'article 2, point a), du règlement. En effet, comme l'indique la notification, les données à caractère personnel des utilisateurs de l'internet sont collectées et traitées ultérieurement. Cela couvre les adresses IP, les URL consultées, la date et l'heure, les données relatives au trafic internet, etc. Même si le trafic et d'autres données relatives à l'utilisation des communications électroniques ne sont pas directement associés à un utilisateur précis, l'anonymat peut toujours être levé si l'ERA décide d'effectuer une enquête approfondie en recoupant les contenus des journaux internet et ceux d'autres systèmes de l'ERA. Les personnes concernées sont donc identifiables.

Dans ses communications ultérieures avec le CEPD, l'ERA a clarifié la situation en indiquant que le contrôle des journaux internet était automatisé et «*anonyme*» dans la mesure où elle a précisé que les adresses IP sont générées dynamiquement aux clients et qu'elle ne consigne sur aucun dossier les informations relatives à l'affectation ni la génération d'adresses IP (journaux DHCP). Par conséquent, selon l'ERA, il est impossible de retrouver l'ordinateur précis auquel correspondent toutes les informations de contrôle de l'internet. Toutefois, le CEPD pense que l'ERA pourrait utiliser d'autres journaux (par exemple, les journaux de messagerie électronique, les journaux d'IAM...) pour établir des corrélations avec les informations contenues dans les journaux internet afin de retrouver la majorité des accès de chacun à l'internet. Si l'absence de journaux DHCP signifie qu'il se peut que certains des accès à l'internet ne soient pas faciles à retrouver, le fait est que, dans la pratique, d'autres journaux de l'ERA fourniront suffisamment d'informations pour déterminer quel utilisateur avait une adresse IP donnée à un moment donné.

Deuxièmement, comme décrit dans la politique internet et d'autres documents, les données à caractère personnel collectées font l'objet d'opérations de *«traitement automatisé»*, telles que définies à l'article 2, point b), du règlement. Toutes les données sont recueillies et analysées à l'aide de procédés automatisés. Un sous-ensemble spécifique de données peut également être analysé manuellement par l'administrateur des systèmes lorsqu'une analyse plus poussée est nécessaire, par exemple en cas de contenu présumé dangereux tel que des virus et similaires. En effet, dans de tels cas de figure, les informations personnelles sont d'abord collectées de manière automatisée directement auprès des utilisateurs de l'internet (enregistrement automatique des fichiers journaux) et analysées ensuite par l'administrateur des systèmes TIC.

En dernier lieu, le traitement est réalisé par une institution/agence/organe communautaire, en l'espèce par l'ERA, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement). Par conséquent, toutes les conditions d'application du règlement sont réunies.

3.1.2. Motifs justifiant un contrôle préalable

L'article 27, paragraphe 1, du règlement prévoit que «*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*» soient soumis au contrôle préalable du CEPD. Le traitement des données dans le cadre des réseaux de communication présente des aspects particuliers en matière de protection des données, qui ont conduit à la rédaction d'un chapitre spécialement consacré à ces aspects (Chapitre IV). En particulier, l'article 36 prévoit le principe fondamental de confidentialité des communications et l'article 37 les dispositions concernant les données relatives au trafic.

L'attention spéciale portée à de telles données doit être considérée comme constituant un risque particulier au sens de l'article 27, paragraphe 1.

L'article 27, paragraphe 2, du règlement contient une liste des traitements susceptibles de présenter de tels risques. Cette liste comprend, sous le point (a), «*les traitements de données*

relatives à la santé et les traitements de données relatives à des suspicions, infractions...» et, sous le point (b), «*les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement*».

Bien que les personnes concernées ne soient pas directement identifiées pendant le contrôle général, - mais lors d'une seconde étape - le contrôle individuel (voir l'approche progressive, point. 3.2.2.) de l'utilisation de l'internet telle que décrite dans les documents de politique pourrait conduire à l'analyse du comportement des utilisateurs (afin de déterminer si leur utilisation de l'internet est conforme à la politique internet), un tel contrôle pouvant nécessiter la collecte de données relatives à des suspicions (si l'on suspecte un comportement illicite) ainsi que d'autres types de données sensibles. En principe, un tel contrôle et les traitements de données connexes doivent faire l'objet d'un contrôle préalable conformément à l'article 27, points a) et b), du règlement.

Le contrôle préalable aux termes de l'article 27 du règlement devrait en principe avoir lieu avant le début du traitement. Le CEPD regrette vivement que, en l'espèce, la notification ne lui ait pas été soumise avant le début des traitements.

3.1.3. Date de notification et date d'échéance pour l'avis du CEPD

La notification a été reçue le 10 février 2012. Le délai dans lequel le CEPD doit rendre son avis en vertu de l'article 27, paragraphe 4, du règlement a été suspendu de 180 jours afin d'obtenir des informations complémentaires.

Par ailleurs, le 10 mai 2012, le CEPD a décidé en vertu de l'article 27, paragraphe 4, du règlement de proroger de deux mois de plus le délai qui lui est imparti compte tenu de la complexité et du caractère délicat du dossier ainsi que du développement parallèle par le CEPD de lignes directrices horizontales sur la question du contrôle électronique.

L'avis doit donc être rendu au plus tard le 10 décembre 2012.

3.2. Licéité du traitement

Le traitement de données à caractère personnel n'est possible qu'en application des motifs visés à l'article 5 du règlement. L'article 5, point a), 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* (…)».

Afin d'établir si le traitement est conforme à l'article 5, point a), du règlement, deux éléments doivent être pris en considération: premièrement, si le traité ou d'autres actes législatifs prévoient une mission d'intérêt public sur la base de laquelle le traitement des données est effectué (*base juridique*) et, deuxièmement, si les traitements sont effectivement nécessaires à l'exécution de cette mission, c'est-à-dire à la réalisation des objectifs poursuivis (*nécessité*).

3.2.1. Base juridique

Premièrement, le CEPD note que le règlement porte en lui diverses dispositions pertinentes aux fins de l'évaluation de la licéité du contrôle, entrepris par l'ERA, de l'utilisation de l'internet. En particulier, le considérant 30 du règlement stipule «*[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 expliqué ci-dessus, l'une

des raisons pour lesquelles l'ERA entreprend un contrôle de l'internet est d'empêcher que ces outils soient utilisés en violation du droit, de politiques de l'ERA ou d'une autre façon non autorisée.

Qui plus est, l'article 35 du règlement stipule que «*Les institutions et organes [communautaires] prennent les mesures techniques et organisationnelles appropriées afin de garantir la sécurité d'utilisation des réseaux de télécommunications et des équipements de terminaux*». Cela justifie le traitement de données de télécommunication qui est nécessaire afin d'assurer la sécurité des systèmes de télécommunication.

Par ailleurs, l'article 37, paragraphe 2, du règlement ajoute un motif juridique supplémentaire habilitant l'ERA à procéder à un traitement de données très spécifique, à savoir à conserver les données relatives au trafic, en l'espèce, les fichiers journaux. En particulier, l'article 37, paragraphe 2, dispose que les données relatives au trafic peuvent être traitées aux fins de la gestion du budget télécommunications et du trafic, y compris aux fins de la vérification de l'usage autorisé des systèmes de télécommunication. La notion de «*vérification de l'usage autorisé*» est essentielle dans la mesure où elle concerne l'usage éventuel de données relatives au trafic à d'autres fins que celle de la gestion du budget et du trafic. Elle permet notamment l'utilisation de données relatives au trafic pour assurer la sécurité du système ou des données et le respect du statut ou d'autres dispositions, telles que celles contenues dans la politique internet.

Deuxièmement, le CEPD note que, en qualité d'employeur, l'ERA a certains devoirs et certaines obligations découlant du droit du travail qui peuvent être considérés comme des motifs juridiques suffisants susceptibles de justifier un traitement proportionnel. Par exemple, le fait que l'ERA ait le devoir de se prémunir contre toute responsabilité découlant des actes de ses employés peut également justifier le traitement. Cela peut inclure le traitement de données sensibles dans certaines circonstances (voir le point 3.3)

Enfin, le CEPD note que les documents émis par l'ERA à propos de ses politiques constituent un autre facteur dont il faut tenir compte afin de déterminer s'il existe un motif juridique suffisant aux fins de l'article 5, point a), du règlement dans la mesure où ils définissent des règles concernant le contrôle des ressources électroniques pour, entre autres, veiller à la sécurité et à la vérification de l'usage autorisé.

3.2.2. Nécessité

Comme indiqué plus haut, l'un des principaux objectifs déclarés de ce traitement est de vérifier si les utilisateurs de l'ERA utilisent les services de TIC conformément aux usages autorisés tels que définis dans les documents de politique interne de l'ERA. Le CEPD note que l'ERA estime qu'il est nécessaire qu'elle opère un certain degré de contrôle de l'utilisation de ses services de TIC, y compris des systèmes internet, afin d'être en mesure d'empêcher ou de détecter les violations de ses politiques ou les atteintes à la sécurité. Par conséquent, il semble qu'un enregistrement sélectif et proportionné des fichiers journaux et leur analyse, à tout le moins dans une certaine mesure, soient jugés nécessaires à l'exécution de la mission consistant à assurer un usage conforme à la politique internet et, partant, la sécurité globale des ressources de TIC de l'ERA.

Un certain contrôle est également jugé nécessaire pour permettre à l'employeur, en l'espèce l'ERA, d'exercer, le cas échéant, ses devoirs et obligations en matière de droit du travail. À titre d'exemple, si l'ERA n'était pas en mesure de surveiller l'utilisation faite par une personne soupçonnée d'avoir un comportement contraire à sa politique (par exemple, le téléchargement de pornographie), elle pourrait ne pas ne disposer des preuves nécessaires pour engager une procédure disciplinaire.

Compte tenu de ce qui précède, le CEPD est d'avis que le contrôle déclaré de l'utilisation des TIC est nécessaire à la réalisation des objectifs visés de la politique. Par conséquent, le CEDP estime

que les exigences de conformité avec l'article 5, point a), du règlement sont satisfaites sur le plan théorique.

Cela étant, il convient de relever qu'un contrôle généralisé ou un contrôle très approfondi de l'utilisation faite de l'internet par chaque utilisateur n'est pas justifié. Dans les cas où le responsable de la sécurité informatique a motif de soupçonner une personne d'abus, le CEPD recommande la mise en place d'une politique consistant à accroître *progressivement* le contrôle en fonction des circonstances. Cela permettra d'éviter que le contrôle soit excessif, puisque seules seront traitées les données nécessaires à la réalisation des objectifs poursuivis. Si les journaux internet font ressortir un abus éventuel des services internet de l'ERA, il serait envisageable, dans un premier temps, de rappeler au personnel les politiques en vigueur et le risque de procédure administrative; si les journaux internet font ressortir un abus continuel de ce type, l'ERA pourrait alors ouvrir une enquête administrative et lancer un contrôle sélectif suivant une méthodologie documentée dans les règles de l'art (voir aussi le chapitre 3.4). Ainsi, un contrôle individuel de l'utilisation de l'internet ne devrait uniquement avoir lieu en cas de soupçon fondé corroboré par des preuves initiales et dans le cadre d'une enquête administrative. L'anonymat du suspect présumé ne pourra être levé que dès lors que la hiérarchie décide d'ouvrir une enquête administrative.

Une procédure claire devrait être mise en place à cet égard en prévision de cette démarche progressive. En cas de soupçon, le directeur informatique pourra par exemple décider qu'il faut faire part dudit soupçon à la hiérarchie concernée (par exemple, le DRH). Cette dernière pourra alors décider d'entreprendre des recherches supplémentaires, à savoir décider de lever ou non l'anonymat dans le cadre d'une enquête administrative.[7]

Le CEPD rappelle que la réalisation d'une enquête administrative relève d'un traitement à caractère général: les enquêtes administratives et les procédures disciplinaires[8]. Ce traitement devrait au préalable être vérifié par le CEPD dans la mesure où il a pour objet d'évaluer le comportement de la personne concernée (article 27, paragraphe 2, point b)) et sous-entend le traitement de données relatives à des suspicions (article 27, paragraphe 2, point a)).

Par conséquent, dans le cadre du contrôle de l'utilisation de l'internet, l'ERA doit en toute circonstance respecter les principes de nécessité et de proportionnalité conformément au principe de qualité des données.

3.2.3. Fichiers journaux des échecs de connexion à l'internet

La politique internet de l'ERA stipule que les fichiers journaux des échecs de connexion à l'internet «*ne seront pas utilisés pour contrôler les comportements individuels sauf dans les cas énoncés à l'article 20 du règlement relatif à la protection des données*». L'article 20 du règlement prévoit des exemptions et limitations, notamment, au principe de qualité des données (article 4 du règlement) dès lors que ces exemptions et limitations constituent une nécessité afin de pouvoir mener, entre autres, des enquêtes criminelles ou une mission de contrôle, d'inspection ou réglementaire liée, même à titre occasionnel, à l'exercice de l'autorité publique.

Comme indiqué dans un avis antérieur,[9] le CEPD estime que les technologies de filtrage sous-entendent une approche préventive contre l'usage abusif de l'internet plutôt qu'une approche

[7] Voir par ex. l'avis du CEPD du 10 novembre 2008 – Contrôle de l'internet par la Cour des comptes (C 2008-284), disponible sur le site du CEPD.
[8] Voir les lignes directrices du CEPD: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-04-23_Guidelines_inquiries_EN.pdf.
[9] Voir l'avis 2008-284, p. 8-9.

répressive ou d'investigation. De l'avis du CEPD, dès lors que l'accès à un site internet est bloqué, le contrôle et la répression du simple fait de tenter d'accéder à ces sites iraient au-delà de ce qui est nécessaire pour atteindre l'objectif visé. Si la personne ne réussit jamais à accéder et à visualiser le contenu d'un site internet bloqué donné, il ne semble pas y avoir une nécessité légitime de traiter cet échec.

Dans le cadre de la procédure, l'ERA a déclaré que les tentatives d'accès à des sites internet bloqués n'étaient pas enregistrées à des fins de répression/contrôle. En effet, les seuls objectifs consistent à évaluer l'efficacité des filtres (à savoir, en l'absence de journal consignant les accès bloqués classés par catégorie il est impossible de déterminer si le filtre marche ou non) et à autoriser l'accès à des sites dont le classement est erroné qui sont bloqués de façon injustifiée.

Dans la mesure où il s'agit là des seuls objectifs, le CEPD recommande d'enlever de la politique internet l'exception relative au contrôle des échecs de connexion dans les cas cités à l'article 20, paragraphe 1, du règlement.

3.3. Traitement portant sur des catégories particulières de données

Le contrôle de l'utilisation de l'internet peut faire ressortir des données à caractère personnel «sensibles». 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). Par exemple, l'appartenance syndicale peut être révélée en accédant à des journaux qui font transparaître qu'un fonctionnaire accède régulièrement au site internet d'un syndicat particulier. Le traitement de données sensibles est, en principe, interdit à moins que l'une des exceptions visées à l'article 10 du règlement soit applicable.

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'utilisation de l'internet peut être jugé nécessaire pour que l'ERA assure la sécurité du système ou des données et le respect du statut et d'autres dispositions. Ceci inclut le respect des devoirs et obligations en matière de droit du travail, tel que le droit de l'ERA d'empêcher la consultation d'informations sexuellement offensantes sur le lieu de travail, ce qui justifierait le traitement d'informations sensibles, telles que certaines URL consultées, susceptibles de révéler qu'un employé se livre à ce type d'activité. Le contrôle des informations sensibles peut également se justifier dans certains cas pour permettre à l'employeur d'exercer ses droits d'employeur, comme le droit d'engager des procédures disciplinaires contre des employés se livrant à des activités illicites, y compris de les licencier.

3.4. Qualité des données

3.4.1. Adéquation, pertinence et proportionnalité

En vertu de 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 qualité des données.

Les finalités déclarées du contrôle de l'internet sont de veiller à ce que l'utilisation des systèmes et services internet de l'Agence s'inscrive dans des finalités qui correspondent à la

mission de l'agence (vérification de l'usage autorisé) et d'éviter les perturbations et les utilisations abusives des systèmes internet (contrôle sécuritaire). Comme indiqué ci-avant, le CEPD estime qu'un certain contrôle de l'utilisation de l'internet peut être nécessaire pour atteindre ces objectifs. Toutefois, le traitement de données à caractère personnel dans ce contexte ne doit être excessif. Il doit être approprié et proportionnel aux finalités recherchées.

Lors de l'évaluation de la proportionnalité, il faudrait tenir compte de la nature particulière des données traitées dans le cadre du contrôle de l'utilisation de l'internet. Les fichiers journaux consignent de manière très détaillée l'activité de chaque utilisateur sur l'internet, y compris les sites consultés, le nombre de visites, les durées de connexion, le temps passé sur chaque site donné, etc. Aussi les institutions/agences/organes communautaires doivent-ils faire preuve d'une extrême prudence lors du développement de leurs politiques internet et de leur application dans la pratique.

À cet égard, une procédure claire permettant d'appliquer l'approche progressive présentée au point 3.2.2 devrait être mise en place.

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 déjà été examinée (cf. point 3.2). La question de la loyauté est étroitement liée aux informations qui sont fournies aux personnes concernées, un aspect qui sera abordé ci-dessous au point 3.8.

3.4.3. Exactitude

L'article 4, paragraphe 1, point d), du règlement, dispose que les données à caractère personnel doivent être «*exactes et, si nécessaire, mises à jour*» et que «*toutes les mesures raisonnables (soient) 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*». En l'espèce, les données sont essentiellement des fichiers journaux. L'ERA doit prendre toutes les mesures raisonnables pour veiller à ce que les données soient mises à jour et pertinentes. Voir aussi le point 3.8 à ce sujet.

3.5. Conservation des données

Aux termes de l'article 4, paragraphe 1, point e), du règlement, 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.

D'après la notification et la politique internet, les journaux fichiers sont conservés pendant 90 jours après leur collecte. Cela est conforme à l'article 37 du règlement, lequel prévoit des mesures spécifiques pour la conservation des données relatives au trafic et à la facturation, dont les fichiers journaux. L'article 37, paragraphe 2, du règlement (CE) nº 45/2001 stipule que les données relatives au trafic peuvent être traitées aux fins de la gestion du budget et du trafic, y compris de la vérification de l'usage autorisé des systèmes de télécommunication. Cependant, ces données doivent être effacées ou rendues anonymes dès que possible et, 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.

Si le contrôle des fichiers journaux ou des données relatives au trafic la conduit à soupçonner une personne d'avoir enfreint la politique internet, l'ERA est autorisée à conserver les fichiers journaux compromettants. 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*». Selon l'interprétation du CEPD, cette disposition s'applique non seulement aux enquêtes criminelles mais également aux procédures disciplinaires.[10]

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 est à noter que cette mesure ne doit être prise qu'au cas par cas, lorsqu'il existe une suspicion légitime qu'une personne a enfreint la PSI ou le statut et que l'ERA a ouvert une enquête administrative. Il faudra à l'issue des six premiers mois déterminer si les données collectées et la vérification réalisée permettent raisonnablement de justifier la poursuite de l'enquête ou l'ouverture d'une procédure disciplinaire. Les données relatives au trafic pourront être conservées plus de six mois uniquement lorsque la réponse à cette question est affirmative.

3.6. Transferts de données

Les articles 7, 8 et 9 du règlement définissent certaines obligations à respecter lorsque les responsables des traitements transfèrent des données à caractère personnel à des tiers. Les règles varient selon que les données sont transférées à (i) des institutions/agences/organes communautaires (selon l'article 7), (ii) à des destinataires relevant de la directive 95/46 (selon l'article 8), ou (iii) à d'autres types de destinataires (selon l'article 9).

Le CEPD souligne que l'article 7 du règlement prévoit que les données à caractère personnel soient transférées aux fins de «*l'exécution légitime de missions relevant de la compétence du destinataire*». Afin de se conformer à cette disposition, le responsable du traitement est tenu, lorsqu'il communique des données à caractère personnel, de vérifier que *(i)* le destinataire possède la compétence nécessaire et que *(ii)* le transfert est nécessaire.

En l'espèce, le responsable de l'ITFM, l'administrateur des systèmes et le responsable de la sécurité des TIC semblent être les personnes chargées de la gestion interne du contrôle de l'utilisation de l'internet. Le responsable de l'administration est cependant le responsable des traitements relatifs aux enquêtes administratives et procédures disciplinaires. L'ERA doit par conséquent examiner si les transferts allant du responsable de la sécurité des TIC, de l'administrateur des systèmes et du responsable de l'IFTM jusqu'à la liste de destinataires décrite dans les faits est conforme à l'article 7. La nécessité de tels transferts doit être analysée à la lumière de l'approche progressive décrite ci-dessus.

Le CEPD recommande à l'ERA de revoir la liste des destinataires à la lumière de ce qui précède et d'évaluer au cas par cas si les conditions de l'article 7 sont remplies. En particulier, seules les personnes chargées de décider si une enquête administrative doit être ouverte et de lever l'anonymat des données semblent être compétentes au vu de l'Article 7.

Ultérieurement, dans des circonstances particulières, les données peuvent être divulguées de manière temporaire aux catégories suivantes de destinataires au sein des institutions/agences/ organes européens:

- l'OLAF et/ou l'IDOC dans le cadre de leurs enquêtes,

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

- l'Ombudsman, à sa demande,
- le contrôleur européen de la protection des données, à sa demande,
- les juges de la Cour de justice européenne, à leur demande.

Le CEPD estime que les transferts d'information à l'OLAF et/ou à l'IDOC, à la Cour de justice européenne, à l'Ombudsman ou au CEPD aux fins de l'exercice de leurs missions officielles satisfait à ces conditions. Ces destinataires sont, en principe, compétents pour s'acquitter de la tâche pour laquelle les données sont transférées. Il incombe au responsable du traitement d'examiner la question de la nécessité au cas par cas.

Les transferts de données à l'attention du Parquet seront gérés dans le cadre de l'avis de contrôle préalable relatif aux enquêtes administratives et procédures disciplinaires. En effet, un tel transfert n'aura lieu que dans la mesure où l'enquête administrative aboutit à la conclusion qu'un membre du personnel a commis une infraction pénale.

Selon la notification, aucun transfert proposé vers un pays tiers ou à une organisation internationale n'est prévu.

3.7. Droits d'accès et de rectification

Aux termes de l'article 13 du règlement, 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 le caractère obligatoire du droit d'accès, sauf exception, et que l'ERA est tenue de mettre en place les procédures permettant l'exercice de ce droit. Le droit d'accès comprend, notamment, le droit d'être informé et d'obtenir une copie des données traitées relatives à une personne sous une forme intelligible. En l'espèce, l'anonymat des personnes concernées ne sera levé que lorsque l'ERA décidera, en fonction des données collectées dans le cadre du contrôle de l'utilisation de l'internet, d'ouvrir une enquête administrative. Par conséquent, dans la pratique, les droits d'accès et de rectification ne peuvent être exercés avant l'ouverture d'une enquête administrative.

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 la personne que des données la concernant sont collectées et traitées. La personne concernée a également le droit d'être informée, notamment, des finalités du traitement, des destinataires des données et des droits spécifiques qu'elle possède en tant que personne concernée.

Afin de veiller au respect des articles 11 et 12, l'ERA a pris les mesures suivantes:

- les utilisateurs des TIC ont été informés de la procédure de contrôle au moyen d'une note au personnel intitulée «Utilisation des ressources appartenant à l'ERA en matière de TIC»;
- par ailleurs, dans un délai de 30 jours après l'entrée en vigueur de la TIC, tout utilisateur existant devra signer l'«attestation de prise de connaissance par les utilisateurs de l'ERA» («l'attestation»). Les nouveaux utilisateurs devront signer cette même Attestation avant de pouvoir accéder aux ressources de l'ERA en matière de TIC. L'attestation contient une confirmation indiquant que l'utilisateur a lu, compris et accepté les TIC;
- toute la série de documents relatifs aux politiques est disponible sur le site Intranet de

l'ITFM, dans la partie «DRAFT Policies–ERA Consultation» (VERSIONS PROVISOIRES des politiques - Consultation de l'ERA);

- le responsable de la sécurité informatique organisera dans les prochains mois un programme de sensibilisation spécifique s'inscrivant dans le cadre du Programme de sécurité des informations électroniques;
- enfin, les utilisateurs essayant d'accéder à un site internet interdit sont informés du fait que l'accès a été refusé et des motifs du refus (le site fait partie d'une catégorie indésirable, avec mention du nom de la catégorie). Le message indique les motifs du refus d'accès.

Une fois l'approche progressive décrite au chapitre 3.4 mise en œuvre, et si les journaux internet font ressortir un abus potentiel des services internet de l'ERA, cette dernière devra informer les utilisateurs des règles définies dans la politique internet et de la possibilité que l'Agence ouvre une enquête administrative.

3.8.1. Les canaux de communication

Le CEPD souligne que l'ERA doit faire en sorte que le canal choisi pour informer de l'existence du contrôle permette à chacun de prendre note efficacement de son contenu. De l'avis du CEPD, les deux aspects suivants doivent être pris en compte.

Premièrement, afin qu'ils soient informés efficacement et dans un souci de loyauté envers les personnes concernées, les utilisateurs doivent être avisés directement du traitement en cours portant sur leurs données à caractère personnel. Dans la mesure où la majorité des informations sont contenues dans les documents relatifs aux politiques, leur publication sur l'Intranet semble insuffisante, dans la mesure où tous les utilisateurs ne le consulteraient pas spontanément. Si cela n'a pas encore été fait, le CEPD invite l'ERA à envoyer un avis personnel à tous les employés, par exemple un message électronique, contenant un lien renvoyant à la politique de confidentialité et au document relatif à la politique pertinents.

Deuxièmement, les documents pertinents fournissent les informations pertinentes de façon très dispersée; en effet, pour avoir accès aux informations juridiquement obligatoires, l'utilisateur doit lire au moins quatre documents distincts: la note au personnel, la politique de confidentialité, la politique internet, les TIC et l'ECP. Dans certains cas, le rapport entre les divers documents n'est pas explicite.

De l'avis du CEPD, il convient de fournir les informations pertinentes, y compris le contenu des articles 11 et 12 du règlement (CE) nº 45/2001, dans un document unique (plutôt que dans différents documents). Afin d'éviter toute confusion et de clarifier la politique, le CEPD suggère de rassembler toutes les informations concernant le contrôle de l'utilisation de l'internet au sein d'un seul et même document contenant toutes les informations nécessaires (voir 3.8.2. ci-après). Ce document pourrait être complété par une politique de confidentialité à laquelle il ferait clairement référence.

3.8.2. Le contenu de la politique

Les politiques relatives aux TIC ont principalement pour buts d'informer les utilisateurs des usages des TIC qui sont autorisés et interdits, à illustrer le type de contrôle de l'utilisation qui est effectué, et de mettre en évidence les conséquences des usages à mauvais escient ou abus. S'agissant de la politique internet de l'ERA, le CEPD fait les principales remarques suivantes:

- tant les TIC que la politique internet stipulent que les TIC de l'ERA doivent être utilisés à des fins professionnelles officielles et que seul un usage personnel limité est permis, dans la mesure où cela ne porte pas atteinte aux intérêts de l'ERA. Le concept d'«usage personnel limité» n'est pas explicité;
- la finalité du contrôle de l'internet ne semble pas toujours être clairement définie. En particulier, la Politique stipule clairement que le contrôle des historiques peut être effectué dans l'optique de veiller à la fonctionnalité et à la sécurité des systèmes mais ne semble pas clair quant à la vérification de l'usage autorisé. Si le contrôle avait également pour finalité la vérification de l'usage autorisé, le CEPD recommande de clarifier ce point de façon explicite;
- le document n'établit pas de méthodologie claire de contrôle de l'internet. Cela reflète le fait qu'une telle méthodologie n'a pas encore été mise en place (cf. point 3.4.1. ci-dessus), essentiellement du fait que le contrôle de l'internet est essentiellement réalisé de façon anonyme;
- la politique internet indique clairement que la World Wide Web fait partie de son champ d'application de la politique sans mentionner spécifiquement d'autres protocoles (tels que la messagerie instantanée, le FTP...). Le CEPD recommande de clarifier la politique de façon à inclure tous les protocoles internet.

S'agissant de la politique de confidentialité, le CEPD remarque qu'elle ne contient pas toutes les informations exigées aux fins des articles 11 et 12. Notamment, elle ne comporte pas suffisamment d'informations à propos (i) des finalités du traitement, (ii) des destinataires, (iii) des catégories de données, (iv) de l'existence du droit d'accès. Il manque également les informations supplémentaires qui pourraient être considérées nécessaires concernant les circonstances particulières pour assurer un traitement loyal (telles que la base juridique, les délais de conservation, le droit de saisir le CEPD, etc.).

Le CEPD invite donc l'ERA à remédier à ces carences afin que la politique de confidentialité satisfasse aux exigences de l'article 12 du règlement.

3.9. Mesures de sécurité

Aux termes des 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 sont prises notamment afin d'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'ERA a confirmé avoir adopté les mesures de sécurité exigées en vertu de l'article 22 du règlement, lesquelles sont détaillées dans l'EISP. Le CEPD n'a aucune raison de penser que ces mesures techniques et organisationnelles ne sont pas appropriées pour assurer un niveau de sécurité conforme aux risques présentés par le traitement et la nature des données à caractère personnel à protéger.

Le CEPD considère toutefois qu'étant donné que ces historiques sont utilisés non seulement à des fins purement sécuritaires, mais aussi pour l'évaluation du comportement, les mesures de sécurité pourraient devoir être renforcées. Le CEPD recommande notamment les mesures suivantes:

1. revoir régulièrement les évaluations des risques décrites dans l'EISP (cela pourrait être fait dans le cadre du plan de sécurité des informations décrit dans cette politique);
2. s'assurer que les journaux internet sont protégés contre tout accès non autorisé, toute

modification ou tout effacement, même de la part du responsable de la sécurité des TIC et des administrateurs des systèmes informatiques;

3. veiller à ce qu'il soit possible de remonter jusqu'à une personne précise pour chaque accès aux fichiers journaux de l'internet;
4. veiller à ce que tous les accès aux fichiers journaux de l'internet soient justifiés et suivent une procédure documentée appropriée;
5. veiller à ce que les responsabilités relatives à la gestion des incidents de sécurité, aux enquêtes internes et aux investigations soient clairement attribuées à des fonctions précises et suivent des procédures documentées appropriées.

CONCLUSIONS

Le traitement visé dans la notification ne peut être mis en œuvre qu'à condition que les recommandations figurant dans le présent avis soient pleinement prises en compte. Afin de garantir le respect du règlement 45/2001, le CEPD recommande à l'ERA de:

- supprimer de la Politique internet l'exception concernant le contrôle des échecs dans les cas de figure définis à l'article 20, paragraphe 1, du règlement;
- mettre en œuvre une approche progressive relative au contrôle de l'utilisation de l'internet par chaque utilisateur, conformément au point 3.2.2 ci-dessus. En particulier, entreprendre un contrôle individuel de l'utilisation de l'internet uniquement en cas de soupçon fondé corroboré par des preuves initiales et dans le cadre d'une enquête administrative et une fois que les moyens disponibles moins intrusifs ont été mis en œuvre;
- s'assurer que les transferts de données sont conformes à l'article 7 du règlement, par le biais d'une appréciation tangible de leur nécessité;
- conserver les données relatives au trafic pendant plus de six mois uniquement dans la mesure où elles sont nécessaires pour assurer «*la prévention, la recherche, la détection et la poursuite d'infractions pénales*» (conformément au point 3.7.);
- revoir la liste des destinataires conformément au point 3.6 ci-dessus. En particulier, seules les personnes chargées de décider si une enquête administrative doit être ouverte et de lever l'anonymat des données semblent être compétentes à la lumière de l'article 7;
- envisager de regrouper toutes les informations relatives au contrôle de l'utilisation de l'internet au sein d'un seul et même document contenant toutes les informations nécessaires;
- intégrer et/ou clarifier la Politique internet et la politique de confidentialité conformément aux recommandations présentées au point 3.8.2.;
- renforcer les mesures de sécurité ayant trait aux fichiers journaux en veillant à la traçabilité des opérations de traitement et en limitant les accès aux personnes ayant besoin d'en connaître.

Fait à Bruxelles, le 6 décembre 2012

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données