Avis sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Cour des comptes concernant la «procédure d'accès au disque/courrier électronique privé»

Bruxelles, le 18 janvier 2010 (dossier 2009-0620)

1. Procédure

Le 28 septembre 2008, le Contrôleur européen de la protection des données (ci-après le «CEPD») a reçu de la Cour des comptes européenne une demande de consultation en vue d'un contrôle préalable (article 27, paragraphe 3, du règlement (CE) n° 45/2001) d'une procédure d'accès au disque/courrier électronique privé des utilisateurs. Dans le contexte de l'analyse du dossier, le CEPD a effectué un contrôle sur place, dans le cadre d'une inspection plus large menée du 17 au 19 mars 2009. Le CEPD a examiné certains éléments spécifiques en rapport avec la procédure soumise à son contrôle. Dans ses conclusions du 23 juillet 2009 sur la consultation, le CEPD a demandé qu'une notification formelle en vue d'un contrôle préalable lui soit adressée dans les meilleurs délais concernant ce traitement, conformément à l'article 27 du règlement.

Le 28 septembre 2009, le CEPD a reçu du délégué à la protection des données (ci-après le «DPD») de la Cour des comptes européenne la notification en vue d'un contrôle préalable concernant la procédure d'accès au disque/courrier électronique privé (ci-après «la notification»).

La notification était accompagnée de deux annexes. La première annexe contient une nouvelle version de la procédure (modifiée par rapport à la version initiale reçue pour la consultation) et la seconde concerne les nouvelles règles et les meilleures pratiques en matière de sécurité du courrier électronique, adressées au personnel de la Cour des comptes par l'avis au personnel interne du 5 juin 2009. Le CEPD dispose également des conclusions du contrôle réalisé sur place.

Le 27 novembre 2009, le CEPD a transmis, pour observations, le projet d'avis au DPD. Ces observations ont été reçues le 14 janvier 2010.

2. Les faits

Selon le responsable du traitement, la procédure d'accès au disque/courrier électronique privé a été élaborée par la Cour des comptes afin d'être en mesure de réagir face à différentes situations susceptibles de se produire dans le cadre des activités quotidiennes de l'institution. Comme l'expliquait la notification, cette procédure doit s'appliquer à un nombre limité de cas, lorsque des informations professionnelles sont conservées sur le disque privé ou disque

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
E-mail : edps@edps.europa.eu - Site Internet : www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

U: ou dans la messagerie électronique privée de l'utilisateur et que le responsable du traitement en a besoin en l'absence de l'utilisateur.

Selon le responsable du traitement, les **finalités** poursuivies par la procédure sont les suivantes:

- A) protéger les intérêts de la Cour des comptes lorsque l'information est stockée sur le disque U: (disque privé) ou sur le compte de messagerie électronique d'un utilisateur absent et l'information est nécessaire dans l'intérêt du service et ne peut pas être obtenue auprès d'une autre source avant le retour de l'utilisateur;

- B) lorsqu'un utilisateur décède et la famille demande des informations et des documents nécessaires pour répondre à des instances officielles, un établissement scolaire, des factures, par exemple, qui sont stockés sur le disque dur de l'utilisateur ou sur un compte de messagerie électronique. Cette finalité ne concerne pas la question de l'accès des services de la Cour des comptes aux documents professionnels du membre du personnel défunt;

- C) à la demande de l'utilisateur lorsqu'il a quitté l'institution, mais a besoin d'accéder à l'information et aux documents qui sont toujours stockés sur son disque U: ou sur son compte de messagerie électronique (selon la procédure normale, les fichiers sont conservés pendant quatre semaines après le départ d'un membre du personnel de la Cour).

Il convient d'apporter une précision concernant le statut du disque dur privé de l'utilisateur (appelé «disque U» à la Cour des comptes), d'une part, et les comptes de messagerie électronique utilisés à la Cour des comptes, d'autre part.

Comme nous l'avons appris lors du contrôle sur place, la Cour des comptes considère que le «disque U» est un disque privé pour chaque membre du personnel, auquel seul ce membre du personnel doit normalement avoir accès. Par conséquent, l'accès de tiers à ce disque doit être soigneusement limité. Lors du contrôle sur place, le responsable a déclaré qu'il est recommandé aux utilisateurs d'utiliser les disques de réseau S et R pour le stockage des fichiers professionnels, plutôt que le disque de réseau U, qui est réservé à l'espace privé des utilisateurs.

En revanche, les comptes de messagerie électronique sont des comptes professionnels (chaque compte de messagerie se termine par eca.europa.eu). Par conséquent, c'est l'usage privé de cette adresse électronique qui doit être précisément identifié et limité. Le compte de messagerie électronique reste une adresse électronique professionnelle. Ceci est confirmé au point 4.2 des règles et des meilleures pratiques en matière de sécurité du courrier électronique de juin 2009. «*Il est rappelé aux utilisateurs que le matériel informatique et les systèmes de messagerie électronique ont été installés pour un usage officiel. Cependant, l'envoi de messages privés est autorisé pour autant qu'il ne gêne pas l'activité professionnelle*». Il existe donc un droit résiduel d'utiliser le système de messagerie électronique à des fins privées. Il est également souligné au point 4.2 de ce document que «*Pour les communications privées, il est fortement recommandé aux utilisateurs d'utiliser un compte privé externe pour l'échange de messages électroniques privés afin de séparer clairement le travail des communications privées.*»

La **procédure** proposée (décrite dans les annexes de la notification) est la suivante. La personne[1] qui demande l'information stockée, sans nul doute, dans l'espace privé de l'utilisateur spécifié, doit remplir un formulaire type (indiquant, notamment, le motif de la demande d'accès). La demande doit contenir une description détaillée du (des) motif(s) justifiant l'accès, le nom du (des) fichier(s) ou le compte de messagerie électronique et/ou l'objet de l'information. Le formulaire doit être envoyé au responsable de la sécurité de l'information ou, en son absence, au responsable sécurité.

Le formulaire de demande d'accès au disque/courrier électronique privé d'un utilisateur comporte les cases suivantes:

- motif (objet du traitement)
- fichiers/messages électroniques demandés
- origine de la demande + case pour la signature et la date
- cases pour le nom, la signature du DPD et la date
- cases pour le nom, la signature du responsable de la sécurité de l'information et la date
- cases pour le nom, la signature de l'administrateur système et la date.

Le responsable de la sécurité de l'information présente la demande au délégué à la protection des données afin que ce dernier émette un avis écrit à joindre au formulaire de demande. Si l'avis est favorable, le responsable de la sécurité de l'information demande à l'administrateur du système d'accéder, en présence du responsable de la sécurité de l'information, à l'information demandée et de la transmettre au demandeur.

Le responsable de la sécurité de l'information précise, dans le formulaire de demande, quelle information a été fournie et signe le formulaire avec l'administrateur système. Un exemplaire du formulaire de demande complété est envoyé à l'utilisateur concerné et au délégué à la protection des données. Le responsable de la sécurité de l'information conserve l'original du formulaire de demande et l'archive.

Le responsable du traitement souligne, dans la notification, que le traitement présente des risques particuliers, dans la mesure où il existe un risque de violation de la confidentialité des communications. La procédure est mise en œuvre parce qu'une personne autre que le titulaire du compte de messagerie électronique peut avoir accès à des communications stockées dans ce compte de messagerie. Le CEPD observe que la notification fait uniquement référence à une violation de la confidentialité dans le cas de messages électroniques.

Dans le cadre de son inspection, le CEPD a examiné certains éléments spécifiques en rapport avec la procédure et la politique générale du responsable du traitement vis-à-vis des disques privés et de l'utilisation du courrier électronique. Ces éléments sont énoncés ci-dessous.

Les **personnes concernées** par cette procédure sont tous les utilisateurs qui possèdent un disque privé (disque U:) et un compte de courrier électronique à la Cour des comptes.

Les **données** traitées sont les données des utilisateurs et d'autres informations contenues dans les messages électroniques.

Comme l'expliquait la notification, différents motifs/événements peuvent déclencher la procédure. De même, les personnes qui demandent l'accès aux données peuvent varier. La notification indique que l'unité à laquelle appartient l'information demandée (cas A), la

[1] AIPN, directeur RH, responsable hiérarchique direct.

famille du défunt (cas B) et le propriétaire des données (cas C) sont autant de **destinataires** potentiels des données.

Selon la notification et la description faite par le responsable du traitement, on peut considérer que les destinataires sont spécifiques à chacune des trois situations prévues dans le cadre de ce traitement.

S'agissant du **stockage des supports**, les données récupérées sont sauvegardées sur le serveur de fichiers et sur le serveur de messagerie électronique. Pour le stockage des supports, les données récupérées sont toujours stockées sur un support externe portable (clé USB, CD/DVD si le destinataire est le propriétaire ou la famille). Si le destinataire est la Cour des comptes, les données sont stockées sur un disque de réseau partagé professionnel ou sur une messagerie fonctionnelle.

Aucun délai de conservation des données n'est prévu dans la procédure ou dans la notification. Comme l'a également expliqué le responsable du traitement dans ses observations, aucune durée de conservation des données n'est nécessaire parce que dans le cas où le destinataire est la famille du défunt ou le propriétaire, la Cour des comptes ne les conserve pas. Lorsque les données récupérées sont stockées sur un disque de réseau partagé professionnel ou dans une messagerie fonctionnelle, les données récupérées sont considérées comme des données professionnelles à caractère personnel et le délai normal de conservation des données professionnelles est d'application.

En ce qui concerne l'**information** fournie aux personnes concernées, il existe des informations générales et spécifiques. La notification mentionne que les utilisateurs seront officiellement informés de la procédure d'accès par un avis écrit officiel et par la publication de la procédure sur l'intranet de la Cour des comptes. La procédure indique que, «dans la mesure du possible», le consentement de l'utilisateur sera demandé au préalable et, en tout état de cause, lorsque la procédure aura été appliquée, l'utilisateur recevra une copie de la demande officielle et une liste des documents et des messages qui ont été consultés et/ou transférés au demandeur. Il importe déjà à ce stade de souligner que toutes les mesures raisonnables doivent être prises pour obtenir ce consentement sans contrainte (article 13 du règlement (CE) n° 45/2001). La question qui doit être appréciée est surtout celle du caractère raisonnable. Il convient de préciser que, lors du contrôle sur place, les inspecteurs du CEPD ont été informés de l'existence d'une communication interne sur l'utilisation du réseau et des ressources TI, adressée au personnel et disponible depuis 1996.

Eu égard aux **droits** des personnes concernées, la notification indique que les utilisateurs peuvent contacter le responsable de la sécurité de l'information (indépendant du demandeur et servant d'observateur) pour lui demander quels fichiers et/ou messages ont été consultés.

La Cour des comptes a adopté [...] des **mesures de sécurité** concernant le traitement:

[...]

3. Aspects juridiques

3.1. Contrôle préalable

Cet avis en vue d'un contrôle préalable concerne le traitement de données de la Cour des comptes dans le cadre de la procédure d'accès au disque/courrier électronique privé. Le présent avis évalue donc la mesure dans laquelle les traitements décrits plus haut sont

conformes au règlement (CE) n° 45/2001.

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 «*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-dessous, tous les éléments rendant le règlement applicable sont réunis en l'espèce.

Premièrement, la procédure d'accès au disque/courrier électronique privé implique la collecte et le traitement ultérieur de *données à caractère personnel*, lesquelles sont définies à l'article 2, point a), du règlement (CE) n° 45/2001. En effet, comme indiqué dans la notification, les données à caractère personnel des membres du personnel seront consultées, collectées et traitées ultérieurement. Ceci comprend l'identification de l'utilisateur, les données, les fichiers et le courrier électronique de l'utilisateur.

Deuxièmement, comme le précise la notification, les données à caractère personnel collectées font l'objet d'un traitement manuel censé faire partie d'un système d'archivage, ce qui est conforme à la définition visée à l'article 2, point b), du règlement (CE) n° 45/2001. En effet, les données à caractère personnel particulières qui sont récupérées sont analysées par le responsable de la sécurité de l'information et par l'administrateur du système dans le cadre d'un système d'archivage.

Enfin, le traitement est effectué par une institution communautaire, en l'espèce la Cour des comptes, conformément au droit communautaire (article 3, paragraphe 1, du règlement (CE) n° 45/2001). Par conséquent, tous les éléments qui rendent le règlement applicable sont réunis en ce qui concerne le traitement des données aux fins de procéder au contrôle de l'internet.

Raisons d'effectuer un contrôle préalable. L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 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*».

Les contrôles réalisés durant l'inspection ont fait apparaître que, dans le cadre de la procédure d'accès au disque privé (appelé «disque U:» à la Cour des comptes) ou au courrier électronique privé, il existe un risque de violer la confidentialité des communications. En recourant à cette procédure, dans un certain nombre de cas, le disque ou le courrier électronique privé de membres absents du personnel peut être consulté par d'autres membres des services de la Cour des comptes. Cela soulève la question de la confidentialité des données en général. En outre, dans certains cas, cette consultation peut également entraîner une violation de la confidentialité des communications au sens de l'article 36 du règlement (CE) n° 45/2001. Ces situations génèrent un risque particulier au sens de l'article 27, paragraphe 1, du règlement.

Notification et date prévue pour l'avis du CEPD. La notification a été reçue en date du 28 septembre 2009. Le délai dans lequel le CEPD doit rendre son avis en application de l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, a été suspendu pendant une période totale de 48 jours afin de permettre la présentation d'observations sur le projet d'avis du CEPD. L'avis doit donc être rendu au plus tard le 18 janvier 2010.

3.2. Licéité du traitement

Comme expliqué dans la partie factuelle, il existe trois cas spécifiques dans lesquels cette procédure sera appliquée: premièrement, dans le cas d'un utilisateur absent détenant des informations nécessaires à l'intérêt du service et qui ne peuvent pas être obtenues auprès d'une autre source avant le retour de l'utilisateur; deuxièmement, lorsque l'utilisateur décède et sa famille demande des informations et des documents et, troisièmement, lorsque l'utilisateur qui a quitté l'institution demande une copie des données.

Le CEPD interprète ces cas de manière restrictive. En outre, chaque finalité est justifiée par un motif spécifique, qui doit être analysé individuellement.

Conformément au règlement (CE) n° 45/2001, le traitement des données à caractère personnel ne peut être effectué que si l'un des motifs visés à l'article 5 existe. Comme le précise la notification, parmi les différents motifs énoncés à l'article 5, les motifs justifiant le traitement se fondent sur l'article 5, point a), qui prévoit que le traitement des 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*».

Le CEPD n'est pas d'accord avec l'idée que l'article 5, point a), puisse servir de base juridique dans tous les cas. En effet, au vu de la procédure susvisée, le CEPD considère que le premier fondement juridique doit être le consentement de l'utilisateur. L'article 5, point d), dispose que le traitement des données à caractère personnel ne peut être effectué que si «*la personne concernée a indubitablement donné son consentement*».

S'agissant, par exemple, de la troisième finalité de l'accès au disque privé ou au courrier électronique privé d'un utilisateur (à savoir l'utilisateur qui a quitté l'institution, mais qui demande ses données), le traitement reposerait de toute évidence sur l'article 5, point d). En effet, dans ce cas, l'utilisateur aura nécessairement consenti au traitement de ses données pour les recevoir.

Le CEPD est également d'avis que, dans le cas de la première finalité (utilisateur absent dont les informations sont nécessaires à l'institution avant son retour au bureau), le consentement de l'utilisateur pourrait également être obtenu au préalable ou une procédure de sauvegarde pourrait être envisagée. On pourrait aussi envisager que les utilisateurs puissent désigner un collègue/tiers, qui serait chargé d'assister au traitement ou aurait même un accès direct aux données au nom de l'utilisateur, sans lancer la procédure plus complexe prévue. Si elle est adoptée, cette procédure nécessiterait naturellement la modification du mot de passe et la mise en œuvre d'une politique de sécurité adéquate.

Des exemples de ces situations ont été discutés durant le contrôle sur place, comme le cas où un utilisateur qui organise une conférence tombe malade et tous les messages électroniques pertinents (envoyés sur le compte de messagerie de l'utilisateur) doivent être récupérés par le responsable du traitement afin de pouvoir poursuivre l'organisation de l'événement. Le CEPD considère que, dans un tel cas (par exemple, l'organisation d'une conférence), la Cour des comptes devrait prévoir une procédure de sauvegarde ou plus simplement le recours à un compte de messagerie électronique fonctionnel, qui serait accessible à plusieurs membres du personnel. Par l'introduction de cette simple mesure organisationnelle, si un tel cas se présentait, la procédure ne devrait pas être appliquée. Cette mesure est, en partie, prévue au point 4.8 des règles et des recommandations en matière de sécurité du courrier électronique, puisque ce document prévoit une procédure de délégation pour les utilisateurs occupant un

poste d'encadrement.

L'article 5, point a), du règlement 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.

Enfin, en cas de décès d'un membre du personnel (cas B), l'institution ne peut pas présumer qu'un utilisateur souhaitait que ses parents aient accès à son disque/courrier électronique privé. Par conséquent, dans ce cas, le traitement ne peut pas se fonder sur le consentement.

Pour déterminer si le traitement est conforme à l'article 5, point a), du règlement (CE) n° 45/2001, deux éléments doivent être pris en compte. La première question consiste à déterminer si le traité ou d'autres actes législatifs prévoient une mission d'intérêt public sur la base de laquelle le traitement est effectué (*base juridique*) et la seconde si le traitement est effectivement nécessaire à l'exécution de cette mission, c'est-à-dire à la réalisation des objectifs visés (*nécessité*).

Base juridique. Les actes juridiques qui justifient le traitement des données par la Cour des comptes sont les suivants.

Pour commencer, le CEPD relève que la Cour des comptes a adopté de nouvelles règles et des meilleures pratiques en matière de sécurité du courrier électronique. Le document énonce, notamment, les règles et les lignes directrices que doivent suivre les utilisateurs des systèmes de messagerie électronique. Il fixe des règles pour assurer la disponibilité, l'intégrité et la performance des systèmes de messagerie électronique. Il tend également à protéger les données à caractère personnel stockées dans ces systèmes.

S'agissant de la procédure particulière d'accès au disque et au courrier électronique privés, le document traite uniquement du courrier électronique, en disant que: «*Une procédure d'urgence sera mise en œuvre pour les cas où les utilisateurs sont absents et où il existe un besoin légitime d'accéder (sic) en urgence au compte de l'utilisateur à des fins professionnelles. Cette procédure sera, elle aussi, conforme au règlement (CE) n° 45/2001*». Par conséquent, ce document ne concerne que le courrier électronique et pas l'utilisation de disques privés, puisqu'ils ne font pas partie du système de messagerie électronique. L'utilisation de disques de réseau est définie et peut être consultée sur l'intranet de la Cour des comptes, dans le dossier d'accueil de chaque nouvel utilisateur et dans le document sur les politiques de gestion des utilisateurs. Selon la notification, un deuxième document faisant partie de la base juridique du traitement des données est la «Procédure d'accès au disque/courrier électronique privé», qui constituera également l'un des éléments de la politique de sécurité de l'information de la Cour des comptes. En outre, le CEPD est d'avis que la déclaration susvisée aurait dû citer les différents cas où la procédure s'applique.

À la lumière des informations disponibles, le CEPD considère que la base juridique du traitement n'est pas suffisante et manque de clarté. En effet, les nouvelles règles et meilleures pratiques en matière de sécurité du courrier électronique ne couvrent pas l'utilisation des disques à la Cour des comptes. Par ailleurs, la procédure générale d'accès au disque/courrier électronique privé ne s'accompagne d'aucune information complémentaire, puisqu'elle ne couvre pas entièrement le traitement envisagé.

Le responsable des données devrait reconsidérer la politique actuelle en matière de courrier électronique, en tenant compte des observations ci-dessous.

L'institution devrait adopter une base juridique spécifique pour l'utilisation et le stockage de courrier électronique privé et élaborer des lignes directrices solides à l'intention de l'usager en ce qui concerne l'utilisation des ressources du réseau et de la messagerie électronique. Ces lignes directrices devraient:

- contenir des informations sur la nécessité de séparer autant que possible les informations professionnelles et privées en utilisant des meilleures pratiques différentes, telles que l'utilisation d'un dossier protégé par un mot de passe spécifique pour la conservation des messages privés (entrants et sortants), le marquage des messages privés en tant que tels, la suppression des messages privés qui ne sont plus nécessaires, etc.;
- définir plus précisément certains termes. Ainsi, le sens du mot «privé» n'est pas clair eu égard au disque U. Comme le concluait le contrôle sur place, bien que le disque U ait été qualifié de privé, il a été dit, dans le même temps, que des *documents officiels* pouvaient aussi y être stockés. Le disque D local a aussi été qualifié de «privé», mais la différence avec les droits d'accès du disque U n'a pas été expliquée (au cours de l'inspection, le responsable du traitement a déclaré qu'il était simplement recommandé aux utilisateurs de ne pas utiliser le disque D). Par conséquent, la base juridique devrait préciser ce que sont des disques professionnels et un disque privé pour la Cour des comptes;
- informer les utilisateurs des conséquences s'ils n'appliquent pas les meilleures pratiques en matière de courrier électronique professionnel et privé, comme le fait que, en leur absence, il peut être nécessaire d'accéder à leur messagerie électronique lorsqu'un document ou un message électronique particulier doit être consulté de toute urgence et que le responsable du traitement n'a pas d'autre moyen de l'obtenir;
- être communiquées de manière plus visible. Le responsable du traitement devrait communiquer les informations/conseils par écrit, par exemple dans le cadre de la politique générale d'utilisation de la messagerie électronique, et il devrait également la publier de manière visible sur le réseau interne de la Cour des comptes.

Par ailleurs, le responsable devrait inclure dans le document proposé sur la procédure d'accès au disque/courrier électronique privé un chapitre sur l'obligation faite à chaque membre du personnel de différencier les données privées et professionnelles afin d'éviter d'appliquer la procédure. Un lien vers les lignes directrices relatives à l'utilisation des ressources du réseau et de la messagerie électronique devrait être fourni.

Enfin, le responsable du traitement devrait revoir les étapes de la procédure et ajouter des informations et le consentement de l'utilisateur comme base du contrôle en ce qui concerne l'octroi ou non de l'accès. À titre d'exemple, la procédure pourrait être modifiée comme suit: après l'envoi de la demande d'accès au responsable de la sécurité de l'information, ce dernier devrait d'abord tenter de contacter l'utilisateur afin de l'informer et d'obtenir son consentement. Cette action et son résultat (c'est-à-dire si l'utilisateur a été contacté et a donné son consentement) devraient également figurer dans le formulaire de demande d'accès.

Nécessité. Comme indiqué plus haut, la nécessité du traitement des données a un lien direct avec la finalité du traitement. En d'autres termes, la nécessité ou non d'un traitement de données dépend de la finalité du traitement considéré. En l'espèce, pour procéder à cette évaluation, il convient d'examiner la mesure dans laquelle le traitement concernant l'accès aux données de l'utilisateur et leur traitement ultérieur est nécessaire à la réalisation des

finalités poursuivies par la procédure.

Comme expliqué plus haut, dans le cadre de cette procédure, le traitement poursuit un triple objectif: protéger l'intérêt de la Cour des comptes lorsqu'un utilisateur est absent et que l'information est nécessaire dans l'intérêt du service, répondre aux demandes de la famille d'un utilisateur défunt et répondre à la demande de l'utilisateur qui a quitté l'institution.

Compte tenu de ces objectifs, le CEPD est d'avis que l'accès du responsable de la sécurité de l'information de la Cour des comptes (et de son administrateur TI) aux données, dans le cadre de la procédure, ne pourrait être considéré comme nécessaire pour atteindre les objectifs poursuivis par la Cour que si celle-ci peut prouver que le membre du personnel a reçu des informations claires et complètes sur l'utilisation 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.

Il convient également de souligner qu'une telle procédure d'accès ne doit pas être comprise comme s'inscrivant dans une 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 la Cour des comptes doit démontrer, dans son avis écrit, qu'il a analysé cet aspect.

S'agissant du cas du décès d'un membre du personnel, le CEPD souhaite insister sur le fait que d'autres institutions ont déjà proposé d'autres solutions. Certaines institutions ont ainsi prévu la possibilité d'appliquer d'autres procédures en vue de la destruction des fichiers électroniques privés précédemment gérés par le membre du personnel défunt.

En l'espèce, le stockage des données aurait un caractère technique et l'accès de l'institution ne devrait donc pas être autorisé, à moins que les conditions visées à l'article 7 du règlement (CE) n° 45/2001 soient remplies. En ce qui concerne la famille, les conditions fixées par l'article 8 du règlement (CE) n° 45/2001 s'appliquent (voir le point 3.6 ci-dessous).

Dans le cas d'un agent ayant quitté la Cour des comptes, d'autres institutions ont également prévu une procédure spécifique pour le départ d'un membre du personnel. Avant de quitter l'institution, le département TI peut contacter la personne concernée et lui fournir une copie du contenu du disque privé sur un CD/DVD. Il peut également lui demander de vider les disques concernés avant son départ.

En outre, s'agissant des messages électroniques privés, une copie de ceux-ci peut également être fournie à la personne concernée sur CD/DVD. Le personnel serait aussi prié de supprimer les messages privés des comptes de messagerie électronique, de sorte que le compte de messagerie ne contiendrait que les données à caractère personnel que l'institution considérera comme des données professionnelles pendant le reste de la durée de conservation (dans le cas de la Cour des comptes, il s'agirait de quatre semaines supplémentaires). Les membres du personnel doivent également être informés du fait que, si leurs données ont été copiées ou s'ils ont personnellement effacé les données à caractère personnel de leur compte de messagerie électronique, des copies peuvent être conservées pendant un certain temps sur le serveur de l'institution. Cela devrait faire partie des informations fournies aux membres du personnel (voir aussi le point 3.8). Il convient également de veiller à ce que l'institution n'utilise pas ces données, hormis dans le cadre d'une procédure disciplinaire.

La mise en œuvre de cette procédure et de ces mesures spécifiques réduirait grandement les problèmes d'accès aux informations privées d'un membre du personnel, qu'elles se trouvent sur un disque privé ou dans le compte de messagerie électronique, après son départ, dans la mesure où il aurait reçu une copie des données et se serait assuré personnellement que les dossiers sont vides.

Le CEPD est d'avis que de telles solutions pourraient être mises en place par la Cour des comptes afin de limiter au maximum le recours à la procédure.

Le CEPD considère que le responsable du traitement devrait appliquer les mesures susvisées afin de se conformer à l'article 5, point a), du règlement (CE) n° 45/2001.

3.3. Traitement portant sur des catégories particulières de données

Le CEPD considère que la procédure d'accès au disque/courrier électronique privé d'utilisateurs de la Cour des comptes peut également impliquer le traitement[2] de 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, dans certains cas, des utilisateurs peuvent avoir stocké licitement (aux termes de la politique de la Cour des comptes) des messages électroniques ou des documents qui révèlent l'une des données susvisées (un document mentionnant un résultat médical ou faisant état de l'adhésion à un parti politique, des échanges de messages électroniques avec un médecin qui mentionneraient des données relatives à la santé dans l'objet des messages, etc.). Par conséquent, l'accès au disque ou au courrier électronique privé d'un utilisateur peut révéler des données à caractère personnel sensibles. Le traitement des données sensibles est, en principe, interdit, à moins que des raisons justifiant leur utilisation puissent être trouvées, conformément à l'article 10 du règlement (CE) n° 45/2001. Le CEPD considère toutefois que l'accès à des catégories particulières de données devrait normalement survenir de manière incidente (l'accès est donné pour certaines données spécifiques et des catégories particulières de données seraient traitées incidemment).

Après une analyse approfondie des dérogations possibles, une base juridique justifiant le traitement peut être trouvée à l'article 10, paragraphe 2, point b), si «*la personne concernée a donné son consentement explicite à un tel traitement*». Ceci ne s'appliquerait que dans le cas d'un utilisateur qui a quitté l'institution (troisième cas) ou lorsque la personne est absente et ne rentre pas avant que l'information soit nécessaire, mais peut donner un consentement valable (premier cas).

Cependant, dans les autres cas (décès de l'utilisateur ou absence de ce dernier et impossibilité d'obtenir un consentement valable), le CEPD considère que seul l'article 10, paragraphe 4, peut servir de base au traitement de données sensibles. Cette disposition se lit comme suit: «*Sous réserve de garanties appropriées, et pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2 peuvent être prévues par les traités*

[2] Conformément à l'article 2, point b), du règlement, on entend par «traitement de données à caractère personnel» toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la **consultation**, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction» (caractères gras ajoutés).

instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, ***si cela s'avère nécessaire, sur décision du contrôleur européen de la protection des données***» (soulignement ajouté).

Le CEPD considère que le présent avis en vue d'un contrôle préalable, y compris les sauvegardes spécifiques qu'il contient, doit être considéré comme répondant aux exigences de l'article 10, paragraphe 4. Cependant, si l'accès est nécessaire, l'intérêt public important, visé à l'article 10, paragraphe 4, doit être démontré au cas par cas.

3.4. Qualité des données

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.

Par conséquent, il y a lieu de veiller à ce que seules les données adéquates, pertinentes et non excessives soient conservées. Dans ce contexte, l'avis écrit du DPD de la Cour des comptes, qui sera joint au formulaire de demande d'accès, est un élément essentiel pour la vérification de la qualité des données, tout autant que le détail des documents qui ont été consultés. Par ailleurs, le CEPD considère que la distinction entre les données privées à caractère personnel (au sens de la politique de la Cour des comptes) et les données professionnelles à caractère personnel contribue à assurer la qualité des données.

Loyauté et licéité. L'article 4, paragraphe 1, point c), du règlement (CE) n° 45/2001 exige que les données soient traitées loyalement et licitement. La question de la licéité a déjà été analysée plus haut (voir le point 3.2). La question de la loyauté est étroitement liée au type d'informations fournies aux personnes concernées (voir le point 3.8 ci-dessous).

Exactitude. Conformément à l'article 4, paragraphe 1, point c), 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*». En l'espèce, les données incluent les messages électroniques et les fichiers. Le responsable de la sécurité de l'information (ou, en son absence, le responsable de la sécurité des personnes) doit prendre toutes les mesures raisonnables pour que les données traitées dans le cadre de la procédure soient à jour et pertinentes (à cet égard, voir aussi le point 3.8).

3.5. Conservation des données

L'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001 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.

Le principe général veut que les données récupérées des comptes de messagerie électronique et d'un disque privé soient conservées pendant une durée qui n'excède pas celle nécessaire à la réalisation de la finalité pour laquelle elles ont été consultées. Les données doivent ensuite être effacées.

Dans le cas du personnel quittant la Cour des comptes ou du décès de membres du personnel, les données contenues dans les comptes de messagerie électronique et sur le disque privé sont normalement effacées dans les quatre semaines. Dans le cas de fichiers journaux, la même procédure devrait s'appliquer. Cependant, si les journaux ne peuvent pas être détruits dans le délai fixé, parce que le cycle de vie des journaux est plus long, il devrait y avoir une disposition juridique par laquelle l'institution déclare que les journaux ne seront pas utilisés à d'autres fins.

Ils doivent ensuite être effacés ou rendus anonymes dans les plus brefs délais et, en tout état de cause, au plus tard quatre semaines après leur collecte, à moins qu'ils ne doivent être conservés plus longtemps afin d'établir, d'exercer ou de défendre un droit dans le cadre d'une action pendante devant la Cour.

3.6. Transfert de données

Les articles 7, 8 et 9 du règlement (CE) n° 45/2001 énumèrent une série d'obligations qui s'appliquent lorsque le responsable du traitement transfère des données à caractère personnel à des tiers. Les règles diffèrent selon que le transfert est destiné à des institutions ou organes communautaires (conformément à l'article 7), à des destinataires relevant de la directive 95/46/CE (conformément à l'article 8) ou à d'autres types de destinataires (conformément à l'article 9).

Comme cela a été expliqué dans la partie factuelle, les destinataires des données varient en fonction de la finalité du traitement et peuvent être l'unité à laquelle appartient l'information demandée, la famille du défunt ou le propriétaire des données (le membre du personnel).

La plupart des transferts de données susvisés sont destinés à des institutions et organes communautaires et, partant, l'article 7 du règlement s'applique. L'article 7 du règlement (CE) n° 45/2001 impose que les données à caractère personnel soient 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, le responsable du traitement doit s'assurer que *(i)* le destinataire possède les compétences adéquates et *(ii)* le transfert est nécessaire.

Afin de se conformer à la procédure établie et aux recommandations du présent avis, le CEPD considère que le transfert de données à l'unité à laquelle appartient l'information demandée est conforme à l'article 7 du règlement (CE) n° 45/2001.

Dans l'hypothèse où la Cour des comptes doit faire face au décès d'un membre de son personnel, tout transfert de données à la famille du défunt doit être conforme à l'article 8 du règlement.

La nécessité des données pour répondre à des instances officielles, un établissement scolaire, des factures, par exemple, doit être justifiée et la justification doit être jointe au formulaire de demande afin que le DPD puisse évaluer la demande. En outre, cette procédure ne pourrait avoir lieu que dans les quatre semaines suivant le décès du membre du personnel, compte tenu de la durée de conservation des données fixée pour les comptes de messagerie électronique et les disques privés.

Il est à noter que le transfert de données au membre du personnel ayant quitté l'institution (qu'il travaille encore ou non dans une institution européenne) serait couvert par son consentement au traitement.

3.7. Droit d'accès et de rectification

L'article 13 du règlement (CE) n° 45/2001 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 confirmation que les données la concernant sont ou ne sont pas traitées, des informations au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte ou les catégories de destinataires auxquels les données sont communiquées, 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 dérogation, et que la Cour des comptes doit mettre en place les procédures autorisant son exercice par les personnes habilitées. 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. La Cour des comptes doit mettre en place les procédures appropriées afin d'assurer que les utilisateurs pourront exercer leur droit d'accès.

La notification prévoit que les utilisateurs peuvent contacter le responsable de la sécurité de l'information (indépendant du demandeur et servant d'observateur) pour lui demander quels fichiers ou messages ont été consultés. Cette disposition est conforme à l'article 13, point b), du règlement (CE) n° 45/2001. En outre, elle indique également que les utilisateurs seront officiellement informés de la procédure d'accès par un document officiel et la publication de la procédure sur l'intranet de la Cour des comptes. Le consentement de l'utilisateur sera demandé et, en tout état de cause, lorsque la procédure a été appliquée, l'utilisateur recevra une copie de la demande officielle et une liste des documents et messages qui ont été consultés et/ou transférés au demandeur. Comme indiqué plus haut, toutes les mesures raisonnables doivent être prises afin d'obtenir le consentement de l'utilisateur sans contrainte.

À la lumière des éléments disponibles, le CEPD considère que la procédure actuelle est conforme à l'article 13.

L'article 14 du règlement (CE) n° 45/2001 prévoit que la personne concernée a le droit de rectifier les données inexactes ou incomplètes. Dans la mesure où les données seront normalement collectées en l'absence du membre du personnel, voire sans qu'il en soit informé, il est important de veiller à ce que ce droit puisse être exercé rétroactivement par les personnes concernées. Cette possibilité doit être prévue en parallèle à toute autre solution compatible avec le fonctionnement quotidien de l'institution pour rectifier directement les données.

En principe, la Cour des comptes doit reconnaître l'existence de ce droit qui, même s'il n'est pas exercé fréquemment, peut s'appliquer dans un nombre de cas restreint.

3.8. Information de la personne concernée

Conformément aux articles 11 et 12 du règlement (CE) n° 45/2001, 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.

La procédure contient les éléments suivants. Les utilisateurs seront officiellement informés du lancement de la procédure d'accès par un document officiel et la publication de la procédure sur l'intranet de la Cour des comptes. Comme indiqué plus haut, toutes les mesures raisonnables doivent être prises pour obtenir le consentement de l'utilisateur et, en tout état de cause, lorsque la procédure a été appliquée, l'utilisateur recevra par retour de courrier une copie de la demande officielle et une liste des documents et messages qui ont été consultés et/ou transférés au demandeur. La procédure prévoit également que l'utilisateur a le droit de contacter le CEPD à tout moment.

En raison de la procédure décrite, la plupart des informations seront fournies à la personne concernée après le traitement.

Après analyse du formulaire de demande décrit dans la partie factuelle et qui sera remis à la personne concernée, le CEPD tient à formuler les observations suivantes:

- il doit être souligné clairement que la finalité de l'accès doit être motivée dans le formulaire de demande, en fournissant d'autres documents (demande du membre du personnel, éléments fournis par la famille, éléments fournis par l'unité qui démontrent que les fichiers demandés sont stockés sur le disque privé ou dans le compte de messagerie électronique). Il ne suffit pas de résumer ce point sous l'intitulé «Motif» du formulaire de demande pour répondre aux exigences de l'article 11, paragraphe 1, point b), du règlement;

- le responsable du traitement doit ajouter une case dans laquelle doit être présenté un résumé des documents joints au formulaire de demande;

- le responsable du traitement doit ajouter une case dans laquelle doivent être mentionnés les différents destinataires susceptibles de recevoir les données. Il ne suffit pas de faire référence au demandeur d'accès (qui n'est pas, la plupart du temps, le destinataire final des données) pour répondre aux exigences de l'article 11, paragraphe 1, point c), du règlement;
- le responsable du traitement doit ajouter la référence au droit d'accès de la personne concernée dans le cadre de cette procédure.

Enfin, à titre de bonne pratique, le responsable du traitement devrait veiller à ce que l'avis écrit du DPD soit joint au formulaire de demande.

3.9. Mesures de sécurité

Conformément aux articles 22 et 23 du règlement (CE) n° 45/2001, 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 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.

Le responsable du traitement a décrit dans la notification les mesures de sécurité mises en œuvre.
[...]
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.
[...]

Conclusion:

Il n'y a pas lieu de penser que le traitement envisagé viole les dispositions du règlement (CE) n°45/2001, pour autant qu'il soit tenu compte des observations qui précèdent. En particulier, cela signifie que:

- l'institution doit adopter une base juridique spécifique pour l'utilisation et le stockage du courrier électronique privé et élaborer des lignes directrices claires sur l'utilisation des ressources du réseau et de la messagerie électronique à l'intention de l'utilisateur. Cette base juridique doit:
    - contenir des règles relatives à la nécessité de distinguer autant que possible les informations professionnelles et privées;
    - préciser le statut des disques utilisés à la Cour des comptes et, en particulier, préciser ce que la Cour des comptes entend par disque privé et disque professionnel;
    - informer les utilisateurs des conséquences de la non-application des meilleures pratiques en matière de courrier électronique privé et professionnel;
    - être communiquée de manière plus visible;

- le formulaire de demande doit être modifié pour tenir compte des observations contenues dans le présent avis;
- le demandeur doit démontrer un intérêt public important, lorsque l'accès à des catégories particulières de données est envisagé. Cet intérêt sera analysé au cas par cas;
- la procédure ne peut pas être utilisée pour contourner les règles établies par une procédure disciplinaire;

- une durée de conservation des données récupérées doit être fixée et ne doit pas excéder la durée normale de conservation;
- lorsqu'il est impossible de détruire les fichiers journaux dans le délai fixé, l'institution doit veiller à ce qu'ils ne soient pas utilisés à d'autres fins;
- le formulaire de demande doit être complété pour inclure:
    - des pièces justificatives,
    - les éléments visés à l'article 11 du règlement (CE) n° 45/2001;
- Les journaux qui se trouvent sur le serveur des fichiers journaux ne peuvent être accessibles qu'à un tiers comme le DPD (en plus du responsable de la sécurité de l'information et des administrateurs du système).

Fait à Bruxelles, le 18 janvier 2010

[Signé]
Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données