EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices sur les données à caractère personnel et les communications électroniques au sein des institutions de l'Union

Décembre 2015

Synthèse

Pour la majorité de la population, les communications électroniques, telles que le courrier électronique, internet et la téléphonie, occupent une place centrale dans les activités privées et professionnelles quotidiennes.

En effet, les communications électroniques sont aujourd'hui essentielles au fonctionnement efficace de la majorité des organisations, et les institutions, organes, offices et agences de l'Union (les «institutions européennes») ne font pas exception à la règle.

Les présentes lignes directrices ont pour but de fournir aux institutions européennes des conseils et instructions concernant le traitement des informations à caractère personnel dans le cadre de l'utilisation des outils de communication électronique, pour s'assurer qu'elles respectent leurs obligations en matière de protection des données à caractère personnel telles qu'énoncées dans le règlement (CE) n° 45/2001 sur la protection des données applicables aux institutions européennes (le «règlement»).

En principe, les organisations utilisant les communications électroniques traitent les données à caractère personnel de leurs travailleurs, par exemple, dans le cadre de la gestion des services de communication électronique, de la facturation et de la vérification de l'usage autorisé. Dans la plupart des cas, un usage privé limité des équipements de travail est permis de sorte que l'intervention d'un employeur sur l'utilisation des communications électroniques par les travailleurs est susceptible de toucher à des aspects directement liés à leur vie privée.

Les communications électroniques sont donc un sujet complexe, qui requiert des orientations. En outre, ce domaine, l'un des plus dynamiques de la technologie, évolue rapidement. Par conséquent, les présentes lignes directrices adoptent une approche neutre sur le plan technologique et ne préconisent pas de mesures techniques spécifiques. Elles mettent plutôt clairement l'accent sur les principes généraux en matière de protection des données qui permettront aux institutions européennes de respecter le règlement sur la protection des données.

Si les présentes lignes directrices sont en principe destinées aux institutions européennes, toute personne ou tout organisme ayant un intérêt pour la protection des données et les communications électroniques pourrait les trouver utiles; le règlement est similaire à de nombreux égards à la directive (CE) 95/46 relative à la protection des données, qui est transposée dans les législations nationales des États membres de l'Union, ainsi que dans les règles nationales de l'Islande, du Liechtenstein et de la Norvège.

Résumé des recommandations

Ci-dessous figure une liste des recommandations formulées dans les lignes directrices. Le contrôleur européen de la protection des données (CEPD) s'en servira comme liste de contrôle pour évaluer votre respect des obligations énoncées dans le règlement.

Recommandations concernant des opérations spécifiques de traitement de données:

Sur la sécurité des systèmes et la gestion du trafic:

R1: Définissez le contenu des journaux de sécurité et leur durée de conservation en fonction des besoins de votre institution en matière de sécurité

R2: Les données collectées à des fins de contrôle de la sécurité *ne doivent être utilisées qu'à cet* effet

R3: Veillez au caractère anonyme des statistiques établies

Sur la gestion de la facturation et du budget:

R4: Demandez aux prestataires externes de limiter au maximum la quantité de données à caractère personnel fournies aux institutions à des fins de facturation, le cas échéant

R5: Fixez la durée de conservation sur la base des délais de contestation des factures

Sur l'usage autorisé des services de communication électronique:

R6: Adoptez une approche progressive en ce qui concerne la surveillance de l'usage autorisé des services de communication électronique

Sur l'enregistrement de lignes téléphoniques spéciales:

R7: Adoptez une mesure administrative précisant comment et pourquoi les appels téléphoniques doivent être enregistrés

R8: Informez les appelants et le personnel de l'enregistrement (possible) de leurs appels téléphoniques *avant* que celui-ci n'ait lieu

Sur l'accès aux courriels en l'absence du travailleur:

R9: Prenez des mesures de précaution pour réduire le besoin d'accéder aux boîtes aux lettres électroniques personnelles à des fins de continuité des activités

R10: Adoptez une politique d'accès aux boîtes aux lettres électroniques des membres du personnel en leur absence

Sur les enquêtes administratives et les procédures disciplinaires:

R11: Veillez à ce que l'accès aux données des communications électroniques soit couvert par les règles relatives aux enquêtes administratives et procédures disciplinaires

R12: Prévoyez des garanties adéquates lors de la planification d'une surveillance discrète

Recommandations horizontales s'appliquant à toutes les opérations de traitement:

R13: Pour chaque opération impliquant le traitement de données à caractère personnel, assurez-vous que les finalités soient déterminées, explicites et légitimes

R14: Ne collectez et traitez que les données nécessaires à la réalisation de la ou des finalités indiquées

R15: Pour chaque opération de traitement, fixez la durée de conservation des données à caractère personnel

R16: Pour chaque opération de traitement, veillez à ce que les données soient traitées pour la finalité indiquée et qu'elles ne soient pas traitées ultérieurement d'une manière incompatible avec la finalité initiale

R17: Informez les personnes concernées sur le traitement dont leurs données feront l'objet

R18: Veillez à ce que chacun puisse exercer facilement ses droits d'accès et de rectification

R19: Gérez les politiques de votre institution relatives au traitement des données des communications électroniques

R20: Notifiez vos opérations de traitement au délégué à la protection des données
R21: Tenez votre documentation et vos notifications à jour
R22: Mettez en place un processus de gestion des risques correctement documenté pour sécuriser les informations
R23: Prévoyez des clauses en matière de protection des données dans les contrats conclus avec les prestataires de services extérieurs
R24: Surveillez les contractants pour veiller à ce qu'ils mettent correctement en œuvre les clauses prévues par leurs contrats

TABLE DES MATIÈRES

1. INTRODUCTION

1 Les présentes lignes directrices ont pour but de fournir aux institutions et organes de l'Union européenne des conseils et instructions pratiques sur le traitement des données à caractère personnel dans le cadre de leur utilisation des outils de communication électronique, pour s'assurer qu'ils respectent leurs obligations en matière de protection des données telles qu'énoncées dans le règlement.

2 Les présentes lignes directrices s'appuient sur les décisions et avis antérieurs du CEPD (sur les consultations administratives, les contrôles préalables et les réclamations), ainsi que sur les travaux réalisés par le groupe de travail «article 29» (étant donné que les termes et concepts utilisés dans les règles applicables au niveau national et aux institutions européennes sont fortement similaires, le CEPD suit l'interprétation du groupe de travail «article 29», le cas échéant). Lorsque nous ne prenons pas position, le CEPD prend en considération celle définie dans ces autres documents.

3 Les présentes lignes directrices ont été élaborées sur la base d'une expérience de longue date. Elles reposent sur le cadre juridique actuel. Si des modifications des règles relatives à la protection des données applicables aux institutions européennes se profilent à l'horizon, les conseils fournis dans le présent document resteront pertinents. Un changement qui devrait intervenir avec ces nouvelles règles concerne l'accent mis sur l'obligation de rendre des comptes, modification que les présentes lignes directrices anticipent déjà.

4 Si vous suivez les présentes lignes directrices, vous pouvez raisonnablement avoir l'assurance que vous respectez le règlement (CE) n° 45/2001. Le CEPD utilisera les présentes lignes directrices comme norme pour évaluer votre respect du règlement.

5 Si vous utilisez ces lignes directrices en tant que service informatique ou autre service d'une institution européenne, votre point de contact immédiat pour de plus amples renseignements sera votre délégué à la protection des données. Il y en a au moins un dans chaque institution, organe ou agence de l'Union, et celui-ci pourra fournir des orientations plus précises.

6 Les présentes lignes directrices présentent non seulement un intérêt spécifique pour les délégués à la protection des données, les coordinateurs de la protection des données, les services informatiques et les autres services administratifs, mais elles pourraient également intéresser toute personne qui utilise les moyens de communication électronique des institutions européennes (toutes les catégories de personnel, les députés au Parlement européen, les délégués des États membres, les contractants, les visiteurs, etc.).

1.1. Structure

7 Les présentes lignes directrices sont divisées en deux parties: une section comportant des recommandations générales relatives à la protection des données dans le cadre de

l'utilisation des communications électroniques et une autre traitant des préoccupations spécifiques, avec des recommandations plus ciblées. Les deux sections contiennent des exemples pratiques pour illustrer le propos le cas échéant.

Rx: Les recommandations sont mises en évidence dans des encadrés et s'accompagnent d'une explication après chaque encadré.

8 Pour les actions obligatoires, nos recommandations utilisent la terminologie adaptée pour indiquer une obligation: «vous devez», «faites cela», «il faut que vous» ou d'autres tournures impératives.

9 De même, les actions recommandées comme des bonnes pratiques, mais qui ne sont pas obligatoires emploient les formulations «vous devriez», «il convient que vous», etc.

10 Les formulations «Il se peut», «pourrait» et autres formulations similaires font référence à des actions qui sont volontaires ou à des manières tout aussi valables d'atteindre le même objectif.

11 Pour des raisons pratiques, les institutions, organes, bureaux et agences de l'Union sont désignés par les termes «institution», «votre institution» ou «votre agence» dans les présentes lignes directrices, mais s'appliquent de la même manière à tous.

1.2. Champ d'application

12 Conformément au champ d'application du règlement, les présentes lignes directrices s'appliquent au traitement des données *par* les institutions européennes. Dans la plupart des cas, les utilisateurs concernés seront les membres du personnel (ce terme s'entend au sens large et inclut, par exemple, les experts nationaux détachés, les stagiaires et les contractants sur place), mais il peut également s'agir de personnes extérieures aux institutions (par exemple «accès invité» à l'internet). Si les règles spécifiques en vigueur pour les différentes catégories de personnes peuvent varier (par exemple pour les enquêtes administratives auprès des personnes relevant ou non du statut), les principes sont les mêmes. Au final, les lignes directrices s'appliquent lors du traitement, *par* les institutions européennes, des données des communications électroniques relatives à toutes les catégories de personnes concernées, sans préjudice d'une politique séparée ou spécifique que les institutions européennes pourraient appliquer à l'égard de leurs représentants politiques ou à haut niveau.

13 Les catégories suivantes de communications électroniques relèvent des présentes lignes directrices:

- téléphonie, fixe et mobile;
- courrier électronique;
- internet.

14 Les lignes directrices portent sur le traitement des données à caractère personnel produites par les communications électroniques aux fins suivantes:

- gestion de la facturation et du budget;
- sécurité des systèmes et gestion du trafic;
- gestion des incidents et dépannage;
- vérification de l'usage autorisé des systèmes de communication électronique;
- enregistrement des lignes téléphoniques spéciales (par exemple, lignes d'urgence);
- accès aux données des communications électroniques relatives à un travailleur en son absence;
- enquêtes administratives et procédures disciplinaires (EAPD).

15 NE relèvent PAS des présentes lignes directrices:

- les systèmes de gestion de l'identité et des accès;
- le contrôle au moyen de la vidéo-surveillance;
- les sessions à distance sur le réseau de l'organisation;
- les systèmes de surveillance des activités des utilisateurs (comme le contrôle de la productivité);
- le stockage local (par exemple, stockage de dossiers sur les disques locaux);
- les communications entre utilisateurs et entre utilisateurs et serveur sur le réseau de l'organisation (par exemple, messagerie instantanée entre collègues, accès aux sites internet internes, etc.);
- les sites internet institutionnels publics;
- le traitement des données à caractère personnel de tierces personnes lorsqu'elles utilisent leurs appareils mobiles.

2. RECOMMANDATIONS RELATIVES AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL POUR DES RAISONS SPÉCIFIQUES

16 La présente section porte sur des préoccupations spécifiques concernant le traitement des données à caractère personnel dans le cadre de l'utilisation des communications électroniques et contient des recommandations pour répondre à ces préoccupations. Ces recommandations doivent être appliquées en sus des recommandations générales formulées dans la section 3 ci-dessous. Les recommandations générales sont toujours applicables y compris lorsqu'elles ne sont pas mentionnées spécifiquement.

2.1. Sécurité des systèmes et gestion du trafic

17 Il se peut que les communications électroniques de votre institution exigent une certaine surveillance destinée à assurer leur bon fonctionnement. Il s'agit notamment des opérations de traitement dont le but est de:

- garantir la sécurité et la stabilité des systèmes;
- détecter et prévenir les attaques (internes et externes);
- veiller au bon fonctionnement des systèmes;
- mesurer l'utilisation.

18 Une certaine forme de surveillance de l'internet peut également se révéler nécessaire pour garantir la fonctionnalité (contrôle) et la sécurité du réseau.

R1: **Définissez le contenu des journaux de sécurité et leur durée de conservation en fonction des besoins de votre institution en matière de sécurité**

19 Vous devez limiter la surveillance de l'internet à des fins de sécurité et de gestion du trafic à ce qui est pertinent et approprié au regard des finalités du traitement (voir les points 95 et suivants concernant la qualité des données). En pratique, cette recommandation suppose:

- l'utilisation d'autres outils ou technologies moins intrusifs si possible (comme le blocage des pages internet) et la limitation de la création de journaux en conséquence;
- la limitation des informations à caractère personnel enregistrées dans les journaux à celles qui sont absolument indispensables;
- la fixation d'une durée de conservation limitée pour les journaux.

20 Par exemple, les journaux d'accès à l'internet incluent généralement les informations suivantes (par utilisation et par tentative d'accès à l'internet):

- une identification de l'utilisateur et une adresse IP;
- le volume de données échangées avec l'internet;
- la date et l'heure d'accès.

21 De même, le stockage des données relatives au trafic de courrier électronique peut être nécessaire pour les mêmes finalités. Les champs suivants sont le plus souvent inclus par les institutions européennes et peuvent être des références utiles pour votre organisation:

- De:
- Date:
- Identificateur du message:
- À:
- Objet:
- Cci:
- Cc:
- Type de contenu:
- Expéditeur:

22 **Durées de conservation**: les données à caractère personnel ne doivent pas être conservées pendant une durée excédant celle qui est nécessaire aux finalités pour lesquelles ces données ont été collectées ou traitées ultérieurement (article 4, paragraphe 1, point d), du règlement). Lorsque vous avez déterminé la finalité et le type des données dont vous avez besoin, vous devez en fixer la durée de conservation.

R2: **Les données collectées à des fins de contrôle de la sécurité *ne doivent être utilisées au'à cet* effet**

23 Le principe général de **limitation de la finalité** (voir section 3.4 ci-dessous) restreint les utilisations ultérieures des données à caractère personnel qui sont incompatibles avec la ou les finalités initiales. Pour les journaux de sécurité, ce principe est **davantage renforcé** par l'article 6, paragraphe 2, du règlement qui dispose que «les données à caractère personnel collectées exclusivement dans le but d'assurer la sécurité ou le contrôle des systèmes ou des opérations de traitement *ne peuvent être utilisées pour aucune autre finalité*, à l'exception de la prévention, la recherche, la détection et la poursuite d'infractions pénales graves». Comme exemples d'utilisations à des fins de «sécurité et de contrôle», citons: la gestion des incidents, la recherche de virus, l'analyse des violations et l'établissement de statistiques sur l'utilisation des ressources. L'utilisation de ces journaux à des fins d'évaluation du personnel n'est pas autorisée.

24 Le **contrôle des messages électroniques** à des fins d'élimination des virus ou de tout autre logiciel malveillant, ainsi que des spams, est un exemple de traitement à des fins de «sécurité et de contrôle». Il repose principalement sur le filtrage des données relatives au trafic de courrier électronique (volume, type de fichiers joints, en-têtes des courriels, etc.), mais le filtrage automatisé du contenu est également possible, en particulier dans le cas des spams ou de la détection d'un contenu prédéfini. Si le traitement est automatisé au moyen d'outils logiciels spécifiques, l'intervention manuelle peut être requise dans des cas particuliers justifiés par l'administrateur du système.

Example 1: *Filtrage des spams*

Votre institution filtre les courriels entrants pour éviter les spams. Le personnel s'est toutefois plaint que le système ne détectait pas certains messages non sollicités (faux négatifs), tout en bloquant certains messages légitimes (faux positifs).
Afin d'affiner le système, un administrateur du système doit examiner le contenu des messages signalés par les membres du personnel. Dans ce cas, une intervention manuelle peut être justifiée, alors qu'au cours des opérations normales les administrateurs ne devraient pas regarder le contenu des messages, mais se fier au filtrage automatique.

R3: **Veillez au caractère anonyme des statistiques établies**

25 Lorsque les journaux d'accès à l'internet sont analysés (automatiquement ou manuellement) de manière plus approfondie pour **établir des statistiques** et évaluer l'utilisation de l'internet par votre institution (par exemple par le responsable de la sécurité ou d'autres services administratifs), les données doivent être **anonymisées**. Si l'établissement de ces statistiques peut impliquer le traitement de données à caractère personnel, les **résultats doivent être anonymes**.

2.2. Gestion de la facturation et du budget

26 Il peut arriver que votre institution doive traiter des données à caractère personnel aux fins de la gestion de la facturation et du budget des services de communication électronique, comme les factures détaillées des appels téléphoniques.

27 Les données qui sont traitées pour assurer la surveillance de la facturation et des factures **doivent se limiter à ce qui est nécessaire** (conformément au principe de qualité, voir les points 95 et suivants). Les données ci-après sont généralement jugées suffisantes pour assurer la surveillance des appels sur ligne fixe et téléphone mobile:

- nom associé à l'extension téléphonique;
- numéro de l'extension téléphonique;
- numéros appelés (les trois derniers chiffres doivent être supprimés pour garantir le respect de la vie privée si le fournisseur offre cette possibilité);
- date, heure et durée de chaque appel;
- montants facturés;
- volume de données échangé (pour l'accès à l'internet mobile).

28 En revanche, l'**identité de la personne appelée**, les **appels téléphoniques infructueux**, les **appels manqués**, les **appels reçus** et les **sites internet spécifiques visités ne doivent pas être enregistrés à des fins de facturation**. Ce qui précède n'affecte en rien le besoin éventuel de tenir un registre des appels manqués et/ou passés au niveau local, sur l'appareil lui-même.

R4: **Demandez aux prestataires externes de réduire au maximum la quantité de données à caractère personnel fournies aux institutions à des fins de facturation, le cas échéant**

29 Les informations requises pour la gestion de la facturation et du budget proviennent généralement du fournisseur de communications électroniques, en même temps que les factures (pour la téléphonie), ou sont établies par l'infrastructure informatique de votre institution (pour les données relatives au trafic internet et de courrier électronique). Il appartient à votre institution de demander au prestataire de limiter autant que possible les catégories de données incluses dans les factures correspondantes.

30 Tous les champs indiqués au point 2.1 ci-dessus ne sont pas pertinents pour la gestion de la facturation et du budget. Par exemple, les données relatives au trafic de courrier électronique sont probablement sans intérêt pour la facturation, tandis que le volume de données échangé par l'internet peut être utile lorsque l'accès est facturé sur la base du volume sur les smartphones. Seuls les champs indispensables à la gestion de la facturation et du budget doivent être stockés et utilisés.

R5: **Fixez la durée de conservation sur la base des délais de contestation des factures**

31 La durée pendant laquelle vous envisagez de stocker les registres des appels téléphoniques ou autres journaux (la durée de conservation) à des fins de gestion du budget et de la facturation ne peut dépasser le délai prévu pour contester les factures de services de communication (voir article 37 du règlement). Les délais de contestation des factures peuvent varier en fonction des contrats que votre organisation a conclus avec les prestataires de services de communication et les durées de conservation doivent être fixées en conséquence (voir également la recommandation R15).

32 Si vous devez conserver certaines données plus longtemps, par exemple en vertu de règles financières ou à des fins d'audit, **l'accès doit en être limité** aux personnes (ou rôles) directement impliquées dans ces activités.

33 Le raisonnement exposé aux deux points précédents s'applique également si votre institution permet aux membres de son personnel d'utiliser les équipements de communication à des fins privées et leur facture cet usage.

34 Les différentes institutions peuvent utiliser des méthodes différentes pour distinguer les activités privées et professionnelles, par exemple:

- le recensement et la facturation a posteriori des activités personnelles: une institution peut par exemple fixer pour ladite institution un certain volume de données autorisé (sur la base de son utilisation moyenne par le passé), sur les smartphones fournis aux membres du personnel et facturer aux utilisateurs le volume de données dépassant la quantité offerte; pour les appels, le personnel peut être invité à indiquer les appels privés qui doivent être remboursés à l'institution;
- la demande préalable au standard téléphonique pour les appels privés;
- la demande préalable au standard téléphonique pour certaines catégories d'appels (comme les appels internationaux ou les appels vers les téléphones mobiles) et déclarer si l'appel est à caractère professionnel ou privé;
- l'utilisation d'un code pin personnel pour les appels privés.

Example 2: *Remboursement des frais pour les appels téléphoniques privés*

Votre institution autorise l'usage des téléphones de bureau pour les appels privés, à condition qu'ils soient déclarés par l'utilisation d'un code personnel avant de composer le numéro. À la fin de chaque mois, les membres du personnel reçoivent une liste de leurs appels déclarés (sans les trois derniers chiffres du numéro appelé) et sont invités à rembourser les frais occasionnés par ces appels au cours du mois écoulé. Ces relevés sont conservés pendant six semaines sauf si un différend survient au sujet du remboursement, auquel cas ils sont conservés jusqu'à la résolution du différend. Les membres du personnel sont informés de ces règles (qui sont énoncées dans une politique) lors de leur entrée en service auprès de l'institution.

2.3. Usage autorisé des services de communication électronique

35 Votre institution peut adopter des règles ou une politique sur l'usage autorisé des moyens de communication électronique sur le lieu de travail. Cette politique peut

couvrir des thèmes tels que l'accès à l'internet et l'utilisation des téléphones de bureau à des fins privées, la surveillance de l'accès à l'internet et les sites interdits.

2.3.1. Transparence et procédures

36 Le personnel doit être informé du fait que votre institution autorise ou non l'utilisation privée des services de communication électronique qu'elle fournit. Ces informations doivent au minimum être communiquées au moyen de votre politique sur l'usage autorisé (voir également les sections 3.5 et 3.7 ci-dessous sur l'information et la documentation).

R6: Adoptez une approche progressive en ce qui concerne la surveillance de l'usage autorisé des services de communication électronique

37 La surveillance de l'usage autorisé doit être justifiée et suivre une approche progressive. En l'absence d'activité suspecte, aucun contrôle des personnes ne devrait être effectué. Conformément à cette approche, les communications électroniques doivent d'abord faire l'objet d'un contrôle sur la base d'un agrégat anonyme. S'il s'avère nécessaire pour votre organisation de surveiller certains profils, l'identité de chaque utilisateur doit d'abord être masquée et ne doit être accessible qu'en cas de nécessité.

38 Si des situations ou profils anormaux sont constatés (en termes de volume, de taille ou d'autres indicateurs d'activité), votre institution peut progressivement augmenter la surveillance. Par exemple, un avertissement peut d'abord être envoyé au(x) département(s) concerné(s) indiquant qu'un usage inadéquat des moyens de communication électronique a été constaté et qu'il doit y être mis un terme. Si l'utilisation inadéquate cesse à la suite de cet avertissement, il ne sera pas nécessaire d'effectuer une surveillance des personnes. Si elle se poursuit, la surveillance peut être intensifiée.

39 Il n'y a lieu de procéder à l'identification de l'utilisateur que lorsqu'il existe un soupçon concret de faute (comme l'usage inadéquat des moyens de communication électronique) et dans le cadre d'une procédure définie ou d'une enquête administrative (voir exemple 3). Le soupçon ne doit pas être général, mais raisonnable, spécifique et étayé par de premières preuves concrètes. Votre délégué à la protection des données doit être informé de toute situation où votre institution à l'intention de procéder à une surveillance individuelle. Dans ces cas, la ou les personnes concernées doivent en être informées dès que possible, sauf si l'une des exceptions prévues à l'article 20 du règlement s'applique (voir la section 2.6 ci-dessous sur les enquêtes administratives).

40 La décision de procéder à une surveillance individuelle est importante et, partant, les preuves à la base des soupçons de faute, la nécessité d'une surveillance individuelle, les limites de l'enquête et la proportionnalité des moyens utilisés doivent être évaluées et documentées. La décision de surveiller un membre du personnel doit être prise par l'autorité compétente chargée de la procédure ou de l'enquête, au niveau administratif

adéquat, conformément à une politique écrite et publique de votre institution sur l'utilisation des moyens de communication électronique.

41 Votre institution doit pouvoir suivre toutes les étapes menant à une opération de surveillance et il y a lieu de conserver une piste d'audit de tous les processus y afférents. Si le CEPD (ou tout autre organe) remet en cause la nécessité de la surveillance, il recherchera, au cours de l'enquête, des pistes d'audit claires et des évaluations documentées des mesures à mettre en place (voir également la section sur l'obligation de rendre des comptes au point 3.1 ci-dessous).

2.3.2. Accès à l'internet

42 Il est possible que votre institution souhaite établir des listes de sites internet *interdits* ou d'adresses auxquelles l'accès est bloqué, tels que les sites dont on sait ou dont on soupçonne qu'ils diffusent des logiciels malveillants. De même, elle peut souhaiter bloquer l'accès à certains sites internet dépourvus d'intérêt professionnel légitime, comme les jeux en ligne ou la pornographie. Lorsqu'ils tentent d'accéder à ces sites, les utilisateurs doivent être informés du fait que le site est bloqué et de la raison du blocage (à savoir la catégorie à laquelle le site appartient; il n'est pas nécessaire de publier en interne la liste des sites bloqués de manière proactive).

43 En principe, les adresses sources des personnes qui tentent d'accéder aux sites bloqués ne doivent pas être enregistrées; en revanche, les adresses cibles (des sites interdits) peuvent être enregistrées. En règle générale, les adresses sources ne devraient pas être enregistrées aux fins de vérification de l'usage autorisé, sauf s'il existe des preuves concrètes de problèmes de sécurité, comme une hausse soudaine des tentatives de connexion à un site bloqué. Cette approche est conforme au principe de qualité des données (voir point 95).

2.3.3. Utilisation du téléphone

44 Il se peut que votre institution souhaite surveiller l'usage autorisé des téléphones mobiles ou de bureau afin de vérifier si l'usage personnel est excessif ou si le personnel omet frauduleusement de déclarer les appels personnels.

45 Il existe plusieurs manières valables de déclarer un usage privé. Les déclarations a posteriori des appels privés ou l'introduction d'un code pour les appels privés sont des exemples pour les téléphones de bureau (voir le point 34 ci-dessus).

46 La surveillance, par votre organisation, des irrégularités suspectées dans la déclaration des appels privés doit se fonder sur des critères objectifs. En principe, l'institution ne devrait pas procéder à des contrôles généraux, systématiques ou aléatoires des factures. La vérification doit se limiter aux factures dépassant une limite prédéfinie, qui, en comparaison avec la consommation moyenne par travailleur et les tâches spécifiques réalisées, peut être considérée comme excessive. Cette limite doit être fixée et clairement indiquée dans la politique de l'institution concernée.

Example 3: *Politique relative à l'usage privé des téléphones mobiles professionnels*

Votre institution fournit à certains membres du personnel un téléphone mobile à usage professionnel qui peut également être utilisé modérément pour des appels privés.
La politique communiquée aux membres du personnel qui demandent un téléphone professionnel précise qu'un usage personnel limité est autorisé et qu'une attention particulière doit être accordée à l'itinérance. La politique précise également le plafond applicable à une facture mensuelle moyenne; si ce plafond est dépassé, l'utilisateur en sera immédiatement informé par un sms (envoyé par le système) et sera invité à déclarer les appels privés et à rembourser ceux qui dépassent le plafond. Si le plafond est dépassé trois mois de suite, le supérieur hiérarchique du membre du personnel peut en être informé.

47 Si le plafond a été dépassé, le membre du personnel devrait avoir la possibilité de fournir une explication avant qu'une quelconque mesure ne soit prise. À ce stade, l'encadrement ne devrait pas encore avoir accès à la facture détaillée. Si les explications ne sont pas convaincantes, et qu'il subsiste un soupçon raisonnable d'usage non autorisé, une enquête administrative peut être ouverte.

48 Dans ce cas, le travailleur doit immédiatement être informé de l'ouverture de l'enquête administrative, sauf si une exception prévue à l'article 20 du règlement s'applique (voir également le point 113 ci-dessous). Au cours de la phase de vérification, le travailleur peut être invité à justifier des appels privés spécifiques figurant sur la facture et qui sont une source de préoccupation.

2.4. Enregistrement de lignes téléphoniques spéciales

49 Il est possible que votre institution souhaite enregistrer les appels entrants vers certains numéros de téléphone comme les numéros d'assistance téléphonique d'urgence ou de dénonciation. Les enregistrements peuvent être nécessaires pour une ou plusieurs finalités spécifiques, par exemple pour vérifier le contenu d'un message afin que le personnel du numéro d'assistance téléphonique puisse répondre de manière adéquate ou pour servir de support de formation.

Example 4: *Enregistrement des lignes téléphoniques d'urgence*

Votre institution dispose d'une ligne d'assistance téléphonique d'urgence spéciale. Les appels vers cette ligne sont enregistrés. Le membre du personnel chargé d'un appel peut réécouter le message et le stocker comme preuve d'activités opérationnelles. Cette opération peut être nécessaire pour préciser le contenu du message, fournir des preuves lors d'actions judiciaires ou administratives ultérieures ou soutenir la formation du personnel. Les procédures sont définies dans un document approuvé par votre directeur; des affiches sont diffusées au sein de l'institution pour indiquer au personnel qu'il existe une ligne d'assistance téléphonique et que les appels seront enregistrés.

50 Conformément au principe de proportionnalité, les institutions européennes ne doivent pas faire enregistrer *tous* les appels entrants et sortants passant par le standard téléphonique ou par celui des départements. Ce n'est que dans des circonstances

exceptionnelles que l'enregistrement général des appels reçus par un service entier (plutôt qu'une ligne téléphonique spécifique) peut être considéré comme nécessaire. En tout état de cause, votre institution doit être en mesure de montrer pourquoi l'enregistrement de ces appels est *nécessaire* pour remplir sa mission (y compris les opérations). Pour de plus amples informations, voir les dossiers 2005-0376 et 2006-0102 du CEPD disponibles sur notre site internet.

R7: **Adoptez une mesure administrative précisant comment et pourquoi les appels téléphoniques doivent être enregistrés**

51 En l'absence de base juridique spécifique, les modalités de l'enregistrement (les lignes téléphoniques concernées, les durées de conservation, les finalités pour lesquelles les enregistrements peuvent faire l'objet d'une utilisation ultérieure, etc.) doivent être énoncées dans des dispositions administratives adoptées au niveau adéquat.

52 Il n'est toutefois pas suffisant, en soi, d'indiquer que l'enregistrement est *nécessaire à l'exécution des missions* de votre organisation et/ou à sa *gestion et à son fonctionnement* (article 5, point a), et considérant 27 du règlement (CE) n° 45/2001) pour justifier l'enregistrement des appels. Des documents d'information complémentaire doivent être fournis. Cette documentation doit indiquer les raisons pour lesquelles l'enregistrement de ces lignes spécifiques est nécessaire; parmi les raisons possibles figurent le caractère sensible du service fourni, sa nature hautement technique, la volatilité des informations échangées, le besoin éventuel d'y accéder à l'avenir et une probabilité élevée de litige.

53 Si l'enregistrement n'est pas continu, mais qu'il s'effectue dans des circonstances particulières, par exemple lorsqu'une alerte de sécurité est signalée; en outre, la documentation doit également préciser la procédure à suivre pour décider quand l'enregistrement doit être activé.

R8: **Informez les appelants et le personnel de l'enregistrement (possible) de leurs appels téléphoniques *avant* que celui-ci n'ait lieu**

54 Les appelants doivent être informés au préalable que leur appel sera/pourrait être enregistré. Pour ce faire, la meilleure manière consiste à diffuser un message audio préenregistré avant qu'un opérateur prenne l'appel (en ce qui concerne les lignes pour lesquelles la rapidité de prise en charge est primordiale, comme les lignes d'urgence, d'autres manières peuvent être envisagées). Cet avis doit également être mis en évidence en plus du numéro de téléphone dans tout répertoire téléphonique, par exemple sur le site internet de votre institution. De même, le personnel travaillant sur les lignes enregistrées doit en être informé également. Il suffit par exemple de placer une déclaration de confidentialité près du téléphone et/ou dans les instructions que le personnel reçoit lors de son entrée en service.

55 Un message vocal ou un message sur un répondeur peuvent être considérés comme un consentement au suivi du message déposé. Cependant, il ne s'agit pas d'un consentement à l'extension du traitement au-delà de cela.

56 Les lignes de dénonciation des dysfonctionnements sont l'une des catégories les plus sensibles des lignes téléphoniques enregistrées. Étant donné que les appels concernent des allégations d'actes criminels ou d'autres fautes graves, ces lignes doivent être créées avec prudence, lorsqu'il existe suffisamment d'éléments attestant leur nécessité. Pour de plus amples informations, voir l'avis 01/2006 du groupe de travail «article 29» et les lignes directrices à venir du CEPD sur la dénonciation des dysfonctionnements.

2.5. Accès aux courriels en l'absence du travailleur

57 Il est possible que votre institution souhaite accéder au contenu des boîtes aux lettres électroniques des travailleurs en leur absence pour assurer la continuité des activités. Il pourrait par exemple s'agir de travailleurs en congé de longue durée, ayant quitté l'institution ou décédés.

58 Étant donné qu'un usage privé limité est généralement autorisé, un tel accès, éventuellement justifié, constitue une ingérence dans leur droit au respect de la vie privée.

R9:	**Prenez des mesures de précaution pour réduire le besoin d'accéder aux boîtes aux lettres électroniques personnelles à des fins de continuité des activités**

59 Afin de réduire au minimum le besoin d'accéder aux boîtes aux lettres électroniques personnelles en l'absence des travailleurs, il faut veiller à ce que les courriers électroniques concernés soient également accessibles ailleurs. Par exemple:

a. demander aux travailleurs d'enregistrer tous les courriers électroniques concernés dans des dossiers électroniques tels que des systèmes de gestion des documents ou des dossiers ou d'archiver la correspondance dans des dossiers papier;

b. mettre en place des boîtes aux lettres électroniques fonctionnelles pour certains services/unités/secteurs, accessibles à tous les travailleurs concernés. Les destinataires pourraient ensuite être invités à copier toute la correspondance liée aux activités dans ces boîtes aux lettres électroniques;

c. demander aux travailleurs quittant l'institution de fournir des notes de transmission complètes.

60 Ces mesures peuvent contribuer à réduire la nécessité d'accéder aux boîtes aux lettres électroniques personnelles. Il est toutefois possible que l'accès à une boîte aux lettres électronique personnelle reste nécessaire.

R10: **Adoptez une politique si l'accès aux boîtes aux lettres électroniques des membres du personnel est requis en leur absence**

61 Le processus d'accès aux boîtes aux lettres électroniques des membres du personnel en leur absence devrait être énoncé dans une politique. Cette politique peut s'inscrire dans le cadre de règles plus générales de votre organisation et peut également couvrir l'accès aux dossiers papier.

62 Les membres du personnel doivent être informés de cette politique de manière générale comme lors de leur entrée en service auprès de votre institution, éventuellement par l'intermédiaire de la politique d'utilisation de la messagerie électronique, et dans des cas spécifiques, lorsque votre institution envisage d'accéder à leurs comptes de messagerie électronique. L'utilisateur devrait recevoir des explications détaillées sur cet accès, indiquant la nécessité, l'urgence, la nature et l'étendue des informations recherchées. Outre les informations à fournir au membre du personnel en vertu de l'article 12 (voir le point 108), les utilisateurs doivent également être informés de leur droit d'opposition au titre de l'article 18 du règlement.

63 Lorsqu'il est impossible d'entrer en contact avec la ou les personnes concernées ou que cela requiert un effort disproportionné, cette ou ces personnes ne doivent pas être informées (article 12, paragraphe 2).

64 Si, en dépit des mesures de prévention proposées au point 59, l'accès reste nécessaire, votre institution peut accéder à la boîte aux lettres électronique conformément à la politique en vigueur en son sein.

65 Toutefois, l'accès aux courriers électroniques ne peut s'effectuer que sous certaines conditions et moyennant certaines garanties. La politique de votre institution en matière de messagerie électronique doit établir des règles claires qui permettent à l'institution d'accéder aux courriers électroniques dans de tels cas. L'accès doit être progressif; par exemple, il convient d'effectuer une recherche par mots clés et dans les en-têtes avant d'accéder au contenu des messages, en informant le délégué à la protection des données et en conservant des journaux pour pouvoir vérifier la licéité de l'accès.

Example 5: *Accéder à une boîte aux lettres électronique après le départ d'un membre du personnel de l'organisation*

Selon les règles de votre institution, les membres du personnel sont tenus de stocker toute la correspondance pertinente dans un système de gestion des documents. Il s'agit notamment des courriers électroniques internes approuvant les documents, émanant des supérieurs hiérarchiques et destinés à ceux-ci, et de toute autre information nécessaire aux futurs gestionnaires de dossiers. Cette mesure, combinée aux notes de transmission, rend peu probable la nécessité de devoir accéder à la boîte aux lettres électronique de l'ancien travailleur à des fins de continuité des activités.
Si cela se révélait malgré tout nécessaire, l'ancien membre du personnel en sera informé, dans la mesure du possible. Afin d'éviter l'accès au contenu privé, les membres du personnel sont invités à enregistrer la correspondance privée dans un dossier nommé en conséquence, afin qu'il puisse être facilement évité. Conformément aux règles de votre institution, les boîtes aux lettres électroniques des anciens membres du personnel sont supprimées dans les deux mois suivant leur départ.

66 Le consentement ne constitue pas un motif approprié de licéité pour accéder aux boîtes aux lettres électroniques dans la situation susmentionnée. Le motif d'accès à un compte de messagerie est la continuité des activités et le fait que cet accès a été jugé nécessaire et proportionné. Voir l'avis 15/2001 du groupe de travail «article 29», p. 13, et l'avis 08/2001 du groupe «article 29», p. 3, pour de plus amples informations.

67 Une autre situation où l'accès peut être nécessaire est celle dans laquelle on donne accès aux membres de la famille de travailleurs gravement malades; lorsque cet accès est requis pour garantir la protection des intérêts vitaux du membre du personnel en question, l'accès nécessaire doit être accordé, sous réserve des garanties appropriées.

2.6. Enquêtes administratives et procédures disciplinaires

2.6.1. Accès aux données des communications électroniques

68 Les données des communications électroniques peuvent constituer des éléments de preuve utiles dans les enquêtes administratives et procédures disciplinaires, par exemple des courriers électroniques montrant des violations de la confidentialité, des journaux d'accès à l'internet suggérant des manquements aux obligations, etc.

69 La présente section porte sur les enquêtes internes au sein des institutions européennes dans le cadre du statut; la situation peut être différente pour d'autres activités d'enquête fondées sur différentes parties du droit de l'Union, tels que les enquêtes menées par la DG Concurrence de la Commission européenne.

70 Les implications au sens large des enquêtes administratives et procédures disciplinaires du point de vue de la protection des données sont examinées dans les orientations du CEPD du 23 avril 2010 relatives au traitement des données à caractère personnel lors d'enquêtes administratives et de procédures disciplinaires.

71 Dans le cadre de la présente section, le responsable du traitement est l'entité chargée de l'enquête (l'IDOC pour la Commission européenne) et non le responsable du

traitement chargé du système de communication électronique dont proviennent les informations (par exemple DG DIGIT).

72 L'analyse individuelle des communications électroniques ne devrait être effectuée que lorsqu'il existe des *motifs raisonnables de suspecter* des abus. Les faits donnant lieu à la suspicion ne doivent pas forcément être aussi concrets que ceux qui justifieraient une condamnation ou une accusation. Toutefois, il convient qu'une suspicion raisonnable soit fondée sur des faits ou des informations propres à persuader un observateur objectif que l'individu en cause peut avoir accompli l'infraction (voir CEDH, Murray c. Royaume-Uni (14310/88), arrêt du 28 octobre 1994, points 55-63).

R11: **Veillez à ce que l'accès aux données des communications électroniques soit couvert par les règles relatives aux enquêtes administratives et procédures disciplinaires**

73 Le moment auquel les enquêteurs peuvent avoir accès aux données des communications électroniques et les modalités de cet accès doivent être définis dans les dispositions du règlement intérieur de votre institution concernant les enquêtes administratives et les procédures disciplinaires.

74 L'accès aux communications électroniques doit être nécessaire et proportionné au regard de la finalité de l'enquête. L'entité (comme l'IDOC) chargée de mener l'enquête devrait procéder à une évaluation concrète de la nécessité et de la proportionnalité, en définissant de manière précise l'infraction suspectée et l'étendue, personnelle, matérielle et temporelle, de la recherche à entreprendre. Cette évaluation devrait être dûment documentée avant l'ouverture de l'enquête pour permettre un examen judiciaire ou administratif en cas de contestation.

2.6.2. Surveillance discrète

75 Dans certains cas, il est possible que votre institution souhaite recourir à une surveillance discrète, comme la tenue de journaux détaillés de toutes les activités d'un membre du personnel sans l'en informer afin d'obtenir des éléments de preuve de son comportement délictueux.

76 Les procédures de surveillance discrète proposées doivent s'accompagner d'une justification convaincante, d'une analyse d'impact et doivent faire l'objet d'un contrôle préalable. En effet, ces procédures impliquent le traitement de données à caractère personnel relatives à des infractions supposées et évaluent la ou les personnes soupçonnées, et relèvent par conséquent à la fois de l'article 27, paragraphe 2, point a), et de l'article 27, paragraphe 2, point b), du règlement. Dans son avis rendu dans le cadre du contrôle préalable, le CEPD peut imposer, au besoin, des garanties spécifiques en matière de protection des données.

R12: **Prévoyez des garanties adéquates lors de la planification d'une surveillance discrète**

77 En principe, le CEPD rendra un avis favorable dans le cadre du contrôle préalable si toutes les conditions suivantes sont remplies:

- la surveillance discrète s'impose pour enquêter sur une infraction pénale grave dans le cadre d'une enquête judiciaire ou autorisée par les autorités policières des États membres de l'Union, d'autres agents des services répressifs ou par les organes de l'Union chargés des enquêtes;
- le recours à la surveillance discrète respecte la loi et a été formellement autorisé par i) un juge ou tout autre fonctionnaire habilité à cet effet en vertu de la législation de l'État membre de l'Union qui a demandé le recours à la surveillance discrète au sein de votre institution, ou par ii) l'organe de décision supérieur compétent (comme le comité ou le conseil exécutif) de votre institution conformément à la politique écrite et publique de votre institution concernant le recours à la surveillance discrète;
- un registre est tenu, contenant toutes ces autorisations et cas de surveillance discrète. Ce registre doit être accessible sur demande pour examen par votre délégué à la protection des données et le CEPD;
- la surveillance est ciblée en ce qui concerne son champ d'application matériel, personnel et temporel; et à condition
    a. qu'il n'existe pas d'autres solutions que le recours à la surveillance discrète pour enquêter efficacement sur l'affaire; et
    b. les avantages obtenus compensent la violation de la vie privée des personnes surveillées.

2.6.3. Copie-image du contenu des ordinateurs ou d'autres appareils

78 L'investigation informatique peut se définir comme le procédé technique d'inspection des systèmes informatiques et de leur contenu en vue de la collecte, de l'analyse et de la présentation devant les tribunaux de preuves électroniques qui sont solides sur le plan légal et dont la validité et l'intégrité sont dignes de confiance. Les techniques d'investigation informatique permettent également d'extraire les informations cachées, perdues, endommagées ou supprimées (accidentellement ou délibérément) qui peuvent être utiles dans le cadre des enquêtes.

79 Dans la plupart des cas, l'investigation informatique interviendra au cours d'une enquête menée par des organismes tels que l'Office européen de lutte antifraude (OLAF) ou par des autorités nationales dans le cadre d'enquêtes pénales. Par conséquent, pour la plupart des institutions, la question de savoir s'il faut recourir à une investigation informatique et comment la mener revêt un caractère très hypothétique. Dans un souci d'exhaustivité et étant donné que certains aspects de l'investigation informatique sont liés aux présentes lignes directrices sur les communications électroniques, ces aspects sont examinés ci-après.

80 Étant donné que l'investigation informatique est une technique intrusive, elle ne devrait être utilisée qu'en dernier recours et si nécessaire. Pour la même raison, il doit

exister une base juridique solide (traités de l'Union ou un acte juridique adopté sur cette base) pour qu'elle puisse être mise en œuvre.

81 Dans certains cas, les enquêteurs peuvent avoir besoin de disposer d'une copie-image intégrale de l'appareil cible (comme les téléphones, ordinateurs, ordinateurs portables et autres appareils mobiles, etc.) plutôt que de courriers électroniques ou de documents bien précis. Une copie-image peut être nécessaire pour conserver l'intégrité des éléments de preuve collectés. En outre, en fonction des circonstances, les enquêteurs peuvent devoir effectuer des recherches et vérifications complexes sur le matériel saisi, ce qui ne peut se faire sur place. L'existence ou non de cette nécessité dépend en définitive des faits propres à chaque cas.

82 L'acquisition de la totalité du contenu d'un appareil cible est par essence une atteinte à la vie privée. Par conséquent, en tant qu'outil d'enquête, elle ne doit être utilisée que dans des circonstances exceptionnelles, en cas d'absolue nécessité. Les enquêteurs ne doivent pas d'office avoir recours aux copies-images. Des garanties spécifiques devraient être mises en place pour protéger les personnes concernées contre le risque d'abus. En particulier, outre les exigences générales examinées dans la section 2.6.2 ci-dessus, les conditions suivantes doivent être respectées:

- l'entité chargée de l'enquête (OLAF, par exemple) devrait procéder à une évaluation de la nécessité et de la proportionnalité avant d'ouvrir l'enquête et documenter cette évaluation (similaire au point 74). En particulier, elle doit être en mesure de prouver que l'image est nécessaire, c'est-à-dire qu'une autre méthode ne permettrait pas d'établir les faits ou serait considérablement plus complexe;
- des images ou des copies d'ordinateurs ne devraient être prises qu'en cas de soupçon avéré d'une infraction suffisamment grave, confirmée par des preuves préliminaires concrètes;
- les copies-images ne devraient pas être acquises dans le cas d'infractions mineures, lorsque la quantité d'informations à collecter est minime, en cas de demandes de faible importance ou dans d'autres cas où les avantages potentiels de l'enquête ne compenseraient pas le risque d'intrusion dans la vie privée;
- le contenu de l'appareil copié devrait être analysé de manière ciblée. Les processus et les recherches automatisés, par exemple par mots clés, devraient être utilisés pour recenser les données pertinentes pour l'enquête, lesquelles seront extraites et versées au dossier d'enquête. Toute action doit se traduire par une piste d'audit traçable;
- la personne concernée devrait avoir la possibilité, à sa demande, d'être présente lorsque le contenu est copié [dans certains cas, il peut être possible de recourir à des restrictions en vertu de l'article 20 afin de protéger l'enquête (voir points 113 et 114 ci-dessous)], ou d'examiner les fichiers journaux des opérations effectuées sur les données. Elle doit également être informée de son droit d'opposition.

3. RECOMMANDATIONS GÉNÉRALES CONCERNANT LES INFORMATIONS À CARACTÈRE PERSONNEL ET LES COMMUNICATIONS ÉLECTRONIQUES

3.1. Veillez à pouvoir rendre des comptes!

83 L'obligation de rendre des comptes signifie que les organisations doivent respecter leurs obligations en matière de protection des données et être en mesure de démontrer qu'elles le font.

84 Cette notion n'est pas propre aux données des communications électroniques, mais s'applique à toutes les opérations de traitement d'informations à caractère personnel.

85 Toute organisation qui collecte, utilise et stocke (ce que l'on appelle collectivement le traitement) des données à caractère personnel est responsable du respect des règles en matière de protection des données et doit pouvoir rendre des comptes à cet égard.

86 Les institutions européennes traitent des informations à caractère personnel pour de nombreuses raisons, par exemple les activités de passation de marchés et de recrutement, l'évaluation du personnel, la collecte de données relatives à la santé dans les dossiers médicaux, la mise en place de systèmes de gestion du temps, la surveillance vidéo en circuit fermé et l'accès des visiteurs aux bâtiments de l'Union. Par conséquent, les institutions européennes sont responsables du respect des règles en matière de protection des données établies dans le règlement et doivent pouvoir rendre des comptes à cet égard.

87 D'une manière générale, les institutions doivent faire preuve de transparence et être explicites quant à la manière dont elles traitent les données à caractère personnel liées aux communications électroniques et à la surveillance des communications électroniques. Elles doivent documenter leurs politiques et veiller à ce que les utilisateurs en aient connaissance. Le droit au respect de la vie privée existe sur le lieu de travail également et toute personne faisant l'objet d'une surveillance doit en être informée. Les institutions ne peuvent pas partir du principe que le personnel est au courant.

88 Le meilleur moyen pour une institution de pouvoir rendre des comptes consiste à examiner les implications des nouveaux processus du point de vue de la protection des données dès le stade de la conception (**protection des données dès la conception**). Les différents traitements et les différentes technologies exigent des garanties différentes. S'il est associé dès le début du processus, le délégué à la protection des données pourra apporter des conseils et des orientations utiles.

89 Les questions figurant ci-après exposent les principaux points à prendre en considération:

a. **Déterminer la finalité:** Que voulez-vous faire et pourquoi?

b. **Légalité:** Êtes-vous autorisé à le faire?

c. **Limitation de la finalité et sécurité:** Comment ferez-vous pour que les informations à caractère personnel soient utilisées pour les seules finalités prévues?

d. **Droits de l'individu:** Comment informerez-vous les personnes concernées et comment garantirez-vous qu'elles puissent exercer leurs droits (par exemple, déclarations de confidentialité, information ad hoc, accès et rectification, restrictions possibles)?

e. **Documentation et notifications:** Comment documenterez-vous ce que vous faites et comment tiendrez-vous cette documentation à jour?

90 Les points suivants décrivent les éléments minimaux à prendre en considération pour chacune de ces questions.

3.2. Pourquoi avez-vous besoin de traiter les données des communications électroniques et comment allez-vous procéder?

R13: **Pour chaque opération impliquant le traitement de données à caractère personnel, assurez-vous que les finalités soient déterminées, explicites et légitimes**

91 Avant de traiter des données à caractère personnel, il vous faudra **définir à la finalité** pour laquelle vous avez besoin de traiter ces données. Cette finalité doit être **spécifique, explicite et légitime**. Cette analyse est fondée sur les besoins opérationnels de votre organisation et doit être documentée dans les politiques concernées (voir la section3.7 ci-dessous).

92 **Décrivez avec précision** la ou les finalités de sorte que les personnes concernées comprennent les raisons du traitement de leurs données. Des explications claires et concises sont nécessaires. Des indications trop vagues (par exemple, améliorer l'expérience de l'utilisateur) ne sont pas suffisantes sans autre forme d'explication. Pour de plus amples informations, voir l'avis 03/2013 du groupe de travail «article 29» sur la limitation de la finalité, p. 15-16.

93 Une définition **explicite** de la ou des finalités garantit que toutes les personnes concernées par le traitement sont au fait de ce qu'il adviendra (ou non) de leurs données.

94 Les fins **légitimes** sont celles qui sont «conformes à la loi». Dans la pratique, cela implique de disposer d'une base juridique adéquate (voir la section 3.3 ci-dessous) et de respecter les autres exigences en matière de protection des données (telles que des règles spécifiques pour des catégories particulières de données). Pour de plus amples informations, voir l'avis 03/2013 du groupe de travail «article 29» sur la limitation de la finalité, p. 19-20.

R14: **Ne collectez et traitez que les données nécessaires à la réalisation de la ou des**

95 Après avoir défini la finalité du traitement et en avoir démontré la légalité, vous devez vous intéresser à la **qualité des données**. Le principe de **limitation des données**

signifie que vous ne devez traiter que les données dont vous avez besoin pour la ou les finalités déterminées. Conformément à l'article 4, paragraphe 1, point c), du règlement, les données à caractère personnel doivent être «adéquates, pertinentes et non excessives au regard des finalités poursuivies».

96 Cela signifie que vous devez définir quelles sont les informations requises pour atteindre la ou les finalités souhaitées. Si des données ne sont pas nécessaires, vous ne devez pas les traiter. Vous ne devez pas collecter ni conserver d'informations à caractère personnel uniquement parce qu'elles *pourraient* être utiles par la suite. Lorsque ces informations sont conservées pour des finalités diverses, veillez à ce que les intervenants n'aient accès qu'aux données nécessaires à leur rôle dans les opérations de traitement. Par exemple, les membres d'un service d'assistance informatique peuvent avoir besoin d'accéder aux journaux de certains utilisateurs pour répondre aux demandes des utilisateurs, mais ils n'ont pas besoin du même accès qu'un auditeur ou un responsable de la sécurité.

R15: **Pour chaque opération de traitement, fixez la durée de conservation des données à caractère personnel**

97 **Durée de conservation**: Les organisations doivent souvent conserver des informations à caractère personnel dans des dossiers pour certaines finalités (ressources humaines, questions juridiques, etc.). Lorsque vous avez déterminé la finalité et la qualité des données dont vous avez besoin, vous devez en fixer la durée de conservation. Les **durées de conservation** doivent être définies en fonction de l'adage «**aussi longues que nécessaire, aussi courtes que possible**», compte tenu de la ou des finalités du traitement. Conformément à l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel doivent être conservées «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».

98 Lorsque les mêmes dossiers sont conservés pour des finalités différentes, des restrictions en matière d'accès doivent être appliquées en conséquence. Par exemple, le personnel du service d'assistance informatique devra avoir accès aux fichiers journaux récents aux fins du dépannage, tandis que les auditeurs pourraient avoir besoin d'un accès aux fichiers journaux plus anciens; l'accès aux dossiers aux fins de la gestion d'un service et aux fins de l'audit d'un service doit être adapté en fonction des besoins de chaque service.

99 Lorsque seule une partie des données à caractère personnel doit être conservée pendant une période plus longue, vous devez supprimer les données qui ne sont pas nécessaires (par exemple conserver certains journaux pendant une période déterminée, tout en conservant les données sur les comptes d'utilisateur aussi longtemps que ces comptes sont actifs).

3.3. Est-ce légal?

100 Le traitement des données à caractère personnel doit être fondé sur un des motifs prévus à l'article 5 du règlement.

101 La plupart des cas de traitement des données des communications électroniques seront vraisemblablement fondés sur des motifs d'**intérêt public** (article 5, point a)), qui comprend «le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes» (considérant 27). La plupart des bases juridiques pertinentes devraient figurer dans les dispositions du règlement intérieur de votre institution qui régissent «la gestion et le fonctionnement», tandis que l'article 37 du règlement contient des règles spécifiquement applicables aux données relatives au trafic et à la facturation.

102 Le **consentement** des personnes dont les données à caractère personnel sont traitées est un autre motif de licéité [article 5, point d)]. Toutefois, le consentement doit être donné librement, sans que le refus du consentement ne puisse entraîner un préjudice réel ou potentiel. Pour de plus amples informations, voir l'avis 15/2011 du groupe de travail «article 29» sur le consentement.

103 Dans le cadre d'une relation de travail, du fait du rapport de force déséquilibré entre l'employeur et le travailleur, il est peu probable que le consentement puisse constituer une base juridique valable. Par exemple, si votre institution doit avoir accès à la boîte aux lettres électronique d'un travailleur en son absence, le consentement du travailleur ne constitue pas un motif approprié. Cet accès serait plutôt nécessaire pour assurer la continuité des activités dans l'intérêt public. De même, les appels téléphoniques vers les lignes d'urgence peuvent être enregistrés, afin que les opérateurs puissent réécouter l'appel lorsque la compréhension en temps réel se révèle difficile, de façon à dépêcher l'assistance nécessaire; l'appelant et la personne qui reçoit l'appel peuvent ou non avoir consenti à l'enregistrement.

> ***Example 6:*** *Annuaire interne du personnel: nécessité contre consentement*
>
> *Un* annuaire institutionnel *interne contenant, par exemple, le nom, la fonction, l'adresse électronique, le numéro de téléphone et le numéro de bureau peut être «nécessaire pour la gestion et le fonctionnement» d'une institution (article 5, point a) + considérant 27 du* règlement (E*). En l'absence d'un tel annuaire, il serait difficile pour une organisation de fonctionner de manière harmonieuse. Cette nécessité est une justification suffisante pour créer cet annuaire. Si le consentement du personnel n'est pas requis, il est nécessaire de l'informer (voir la section 3.5**Error! Reference source not found.** ci-dessous.*
> *Les photos des membres du personnel ne sont pas une exigence indispensable à l'annuaire; elles ne constituent pas un élément de l'annuaire nécessaire à la poursuite du fonctionnement de de l'organisation. Dans ce cas, le consentement est un motif approprié; vous ne pouvez pas obliger tous les membres du personnel à charger une photo d'eux-mêmes.*

3.4. Les données à caractère personnel ne doivent être utilisées que pour la finalité prévue

R16: **Pour chaque opération de traitement, veillez à ce que les données soient traitées pour la finalité indiquée et qu'elles ne soient pas traitées ultérieurement d'une**

104 La **limitation de la finalité** est l'un des grands principes de la protection des données. Ce principe est conçu pour protéger les personnes en limitant l'utilisation de leurs données à caractère personnel à des finalités prédéfinies, sauf dans des conditions strictes et avec les garanties appropriées. Pour de plus amples informations, voir l'avis 03/2013 du groupe de travail «article 29» sur la limitation de la finalité.

105 Dans certains cas, un **changement de finalité** peut être admis, pour autant que cela soit prévu dans votre règlement intérieur et compatible avec la finalité initiale. Une utilisation ultérieure incompatible avec la finalité initiale n'est possible que dans les conditions prévues à l'article 20 du règlement.

> ***Example 7:*** *Limitation de la finalité et journaux informatiques*
>
> *Une institution européenne conserve des journaux des connexions internet afin d'assurer la fonctionnalité et la sécurité de ses systèmes. L'une des tâches de l'administrateur informatique consiste à veiller au fonctionnement des systèmes. Pour ce faire, elle doit avoir accès à ces fichiers journaux, y compris les sites internet visités par le personnel chaque jour.*
> *La cheffe d'une autre unité demande que l'administratrice lui transmette les fichiers journaux d'un membre du personnel travaillant sous sa supervision, car elle soupçonne ce membre du personnel de passer beaucoup de temps sur des sites de loisirs et sur les réseaux sociaux, négligeant ainsi son travail.*
> *La finalité de la conservation des fichiers journaux est d'assurer le bon fonctionnement des systèmes ainsi que de détecter les incidents et d'y répondre, et non d'aider les membres de l'encadrement à garder un œil sur leur personnel. L'administratrice informatique doit rejeter la demande.*
> *En revanche, si une enquête administrative sur le comportement de ce membre du personnel avait été lancée conformément aux dispositions applicables du règlement intérieur et que la demande émanait du comité d'enquête, le changement de finalité pourrait être autorisé.*

106 Vous devez veiller tout particulièrement à garantir la sécurité des données à caractère personnel qui sont collectées, traitées et stockées. Les organisations doivent prendre les mesures techniques et organisationnelles appropriées pour sécuriser les données afin de tenir compte des risques pour les personnes concernées. Cela suppose, entre autres, de disposer d'un processus de gestion des risques liés à l'information. Pour plus d'informations, voir la section 3.8.1 ci-dessous.

3.5. Le droit de savoir

R17: **Informez les personnes concernées sur le** traitement dont leurs données feront l'objet

107 En règle générale, vous devez informer les personnes concernées sur la manière dont leurs données seront utilisées **avant** le début du traitement.

108 Le contenu minimal des informations qui doivent être fournies est défini aux articles 11 et 12 du règlement. Les personnes concernées doivent être informées des éléments suivants:

a. la personne responsable de traitement (identité du responsable du traitement);

b. la finalité de la collecte, du stockage et de l'utilisation des données;

c. les personnes avec lesquelles les données seront partagées/qui y auront accès;

d. si les données doivent être collectées auprès de la personne concernée: la fourniture des informations est-elle obligatoire ou facultative? Si elle est obligatoire, quelles sont les conséquences de la non-fourniture de celles-ci?

e. si les informations à caractère personnel ne sont pas collectées directement auprès de la personne concernée, l'endroit d'où elles proviennent: quel type de données vont être traitées? C'est par exemple le cas des informations contenues dans les journaux relatifs aux activités sur les systèmes informatiques: étant donné que l'utilisateur ne sait pas ce qui est enregistré, il convient de l'en informer. En revanche, dans une procédure de sélection, il n'est pas nécessaire de répéter, dans la déclaration de confidentialité, l'ensemble des catégories de données demandées dans le formulaire de candidature, étant donné que la personne sait ce qu'elle a fourni; un renvoi au «contenu du formulaire de demande» est suffisant;

f. leur droit d'accès aux données les concernant et de rectification de ces données; il s'agit notamment de fournir des informations sur la manière d'accéder aux données, par exemple, en indiquant les coordonnées de la personne à qui adresser la demande;

g. toute autre information nécessaire pour assurer un traitement loyal des données, telle que:

   i. la base juridique du traitement;

   ii. la durée de conservation des données;

   iii. le droit de recours auprès du CEPD.

109 Vous devez fournir ces informations aux personnes concernées en des **termes concis et aisément compréhensibles**.

110 Vous devez le faire via une **déclaration de confidentialité**, étant donné que les informations contenues dans les documents exposant l'approche de votre institution en matière de traitement des données des communications électroniques ne sont pas rédigées spécifiquement pour informer les personnes dont les données seront traitées. Une simple référence à ces documents ne constitue pas une manière très conviviale d'informer les personnes concernées.

111 Plus une déclaration de confidentialité est courte, plus elle est susceptible d'être lue. Dans la plupart des cas, une page suffira pour communiquer les informations requises. **Les avis «à plusieurs niveaux»** contenant un bref résumé avec un lien vers une explication complète sont également une possibilité.

112 **La publication des déclarations de confidentialité sur le site intranet de l'institution ne suffit pas**. Vous devez activement informer les personnes concernées. Pour le nouveau personnel, l'intégration de ces informations dans le dossier d'accueil peut être une option intéressante; elles peuvent également être communiquées au moyen d'écrans pop-up lors de la première connexion à l'ordinateur.

> ***Example 8:*** *Information sur les règles d'utilisation des ressources informatiques*
>
> *Une institution fournit les services TIC standard à son personnel (téléphones, boîtes aux lettres électronique, accès à l'internet sur les ordinateurs de bureau, accès au WiFi, etc.); les visiteurs peuvent utiliser l'accès WiFi «invité».*
> *Le personnel est informé des règles applicables lors de son entrée en service auprès de cette institution, au moyen du dossier d'accueil, qui comprend une copie du document exposant la politique en la matière et une déclaration de confidentialité concise d'une page (ces documents étant également disponibles sur le site intranet de l'institution). Lorsque la politique est modifiée, les membres du personnel en sont informés par un courrier électronique contenant un résumé des modifications. La politique énonce les règles relatives à la manière dont l'institution peut accéder aux boîtes aux lettres électroniques des membres du personnel en leur absence. En outre, lorsque ces procédures ciblées sont utilisées, les membres du personnel concernés en sont informés personnellement.*
> *Étant donné que seul un petit nombre de ces opérations de traitement présentent un intérêt pour les visiteurs, ceux-ci peuvent être informés d'une manière différente, par exemple au moyen d'une déclaration de confidentialité sur la fiche de renseignements contenant les codes d'accès au WiFi «invité» et/ou par une réorientation vers la déclaration de confidentialité lors de la première connexion au réseau.*

113 Dans certains cas, il peut y avoir de bonnes raisons de ne pas informer immédiatement une personne de l'utilisation de ses données, par exemple dans les premières phases d'une enquête administrative. Le règlement relatif à la protection des données le permet, sous certaines conditions, qui sont énumérées à l'article 20. Pour de plus amples informations, voir les lignes directrices du CEPD sur les droits des individus, pages 26 et suivantes.

114 Il s'agit par exemple de la prévention et de la poursuite d'infractions pénales. Si une institution souhaite recourir à une telle limitation, une documentation exposant en détail les raisons pour lesquelles cette limitation est nécessaire doit être conservée. Dans les cas où ces limitations sont nécessaires, les règles d'application concernant la protection des données au sein de l'institution peuvent exiger la consultation du délégué à la protection des données.

Example 9: *Limitation du droit à l'information*

Un membre du personnel est soupçonné de passer plusieurs heures de sa journée de travail sur des sites web de jeux d'argent et de hasard.
La politique d'accès aux ressources informatiques indique que les fichiers journaux concernant l'accès à l'internet peuvent être utilisés pour des enquêtes administratives et des procédures disciplinaires.
Une enquête administrative concernant le comportement de ce membre du personnel est lancée conformément aux règles applicables. Le fait de l'en informer immédiatement pourrait gravement nuire à l'enquête, dans la mesure où il modifierait probablement son comportement pendant la durée de celle-ci et entraverait ainsi les efforts visant à apporter la preuve qu'il manque à ses obligations.
Dans ces circonstances, le report de l'information peut être justifié. La personne qui dirige l'enquête doit indiquer laquelle des exceptions prévues à l'article 20 du règlement s'applique et pourquoi il est nécessaire d'y recourir. Lorsque la limitation n'est plus nécessaire, le membre du personnel doit être informé.

3.6. Droits d'accès et de rectification

R18: **Veillez à ce que chacun puisse exercer facilement ses droits d'accès et de rectification**

115 Toute personne physique (également connue sous le nom de personne concernée) a un **droit d'accès et de rectification des données à caractère personnel la concernant**, conformément aux articles 13 et 14 du règlement. Votre institution doit uniquement donner accès aux informations dont elle dispose au sujet de cette personne; ces droits **n'obligent pas votre institution à conserver des données qu'elle n'aurait pas conservées autrement**.

116 Les informations que vous êtes tenu de fournir sont précisées dans les lignes directrices du CEPD sur les droits des individus, pages 9 et suivantes. En résumé, vous devez fournir les éléments suivants:

a. si les données à caractère personnel du demandeur font l'objet d'un traitement;

b. des détails sur le traitement, par exemple dans une déclaration de confidentialité et des informations complémentaires le cas échéant;

c. les informations qui sont traitées, et auprès de qui elles ont été obtenues;

d. la logique d'un éventuel processus décisionnel automatisé. Par exemple, si la facture de votre téléphone portable professionnel excède 200 euros, vous recevez un avertissement. Si la facture dépasse 200 euros deux mois d'affilée, votre supérieur hiérarchique en est informé.

117 Le **délai de réponse** légal à une demande d'**accès ou de rectification** au titre du règlement relatif à la protection des données est de trois mois. Toutefois, les modalités d'application concernant la protection des données au sein de votre institution peuvent imposer des délais plus stricts. En cas de doute, vérifiez les délais applicables auprès du délégué à la protection des données.

118 S'il n'est pas possible de procéder à une rectification par la modification des données (par exemple parce qu'il faut préserver l'intégrité des fichiers journaux), le désaccord de la personne concernée doit pouvoir être consigné.

119 Les exceptions à ces droits sont limitées conformément à l'article 20 du règlement relatif à la protection des données. Pour de plus amples informations, voir les lignes directrices du CEPD sur les droits des individus, pages 26 et suivantes.

Example 10: *Octroi de l'accès aux informations*

Une institution autorise les membres de son personnel à utiliser les téléphones de bureau pour leurs appels privés, à condition que ces appels soient déclarés au moyen d'un code spécifique. Le coût de ces appels est pris en charge par le membre du personnel concerné.
L'application utilisée pour collecter ces informations permet aux membres du personnel de vérifier leur propre liste d'appels déclarés, au moyen d'un lien sur le site intranet de l'institution. Si le membre du personnel constate une erreur, un formulaire de contact lui permet d'avertir les responsables, qui procèdent aux corrections nécessaires.

3.7. Documentez ce que vous faites

R19: **Gérez les politiques de votre institution relatives aux données des communications électroniques**

120 L'obligation de rendre des comptes suppose de faire ce qu'il faut de manière responsable et reproductible. Des politiques bien conçues et bien gérées constituent un élément essentiel de l'obligation de rendre des comptes.

121 Ces politiques aident les institutions à voir comment mettre en œuvre les recommandations formulées dans les présentes lignes directrices, telles que celles sur le principe de limitation de la finalité, les principes de qualité des données et l'information de toutes les personnes dont les données à caractère personnel sont traitées.

122 Ces politiques doivent être réexaminées régulièrement et adaptées si nécessaire.

R20: **Notifiez vos opérations de traitement au délégué à la protection des données**

123 Le règlement contient des **obligations spécifiques en matière de documentation**. En vertu de l'article 25, toutes les opérations de traitement doivent être notifiées à votre délégué à la protection des données, qui disposera d'un formulaire à compléter à cet effet. Vous devrez l'informer *avant* le début du traitement, afin qu'il soit en mesure de fournir des conseils, de proposer des améliorations et de notifier le traitement au CEPD en vue d'un contrôle préalable si nécessaire.

124 En outre, **certains traitements présentant un risque** doivent être **notifiés au CEPD** en vue d'un contrôle préalable; pour les communications électroniques, il s'agit essentiellement du traitement de certaines catégories particulières de données mentionnées à l'article 27, paragraphe 2, point a), du règlement et des traitements destinés à évaluer des aspects de la personnalité de la personne concernée (article 27,

paragraphe 2, point b)). Les catégories les plus pertinentes pour les communications électroniques concernent le traitement de données relatives à des suspicions, infractions ou mesures de sûreté. Les mesures de sûreté visées ici ne concernent pas la sécurité de l'information, mais des actions telles que l'admission en traitement psychiatrique forcé, des mesures coercitives prises à l'encontre d'une personne pour sa propre sécurité (ou celles des autres). On citera également comme exemples l'analyse du trafic destinée à évaluer les membres du personnel ou la surveillance discrète dans le cadre d'enquêtes administratives. Le délégué à la protection des données informera le CEPD, mais se mettra en relation avec le responsable du traitement pour remplir le formulaire de notification à envoyer au CEPD. Pour votre propre planification, il convient de tenir compte du délai nécessaire au CEPD pour rendre son avis (jusqu'à 2 mois, pouvant être prolongé pour une période supplémentaire de 2 mois, sans compter la suspension du dossier en cas de demande d'informations complémentaires).

Example 11: *Utilisation des fichiers journaux dans les enquêtes administratives*

Si votre institution met à jour les dispositions de son règlement intérieur relatives aux enquêtes administratives afin de refléter l'utilisation des fichiers journaux dans la procédure, la notification initiale que vous avez transmise à votre délégué à la protection des données en ce qui concerne les enquêtes administratives doit être mise à jour en conséquence. Étant donné que l'utilisation des fichiers journaux n'est pas une finalité en soi mais fait partie des enquêtes administratives, une nouvelle notification séparée n'est pas nécessaire.

125 Voici quelques exemples de traitements qui ne doivent pas être notifiés au CEPD:

a. traitement des données téléphoniques uniquement à des fins de gestion de la facturation et du budget, pour autant qu'il n'y ait aucune intention de vérifier l'usage autorisé ou d'évaluer les travailleurs;

b. traitement des données relatives au trafic (par exemple, courrier électronique et internet) aux fins de la gestion de la sécurité ou du trafic, effectué automatiquement et de manière anonyme, pour autant qu'il n'y ait aucune intention de vérifier l'usage autorisé ou d'évaluer les travailleurs.

R21: **Tenez votre documentation et vos notifications à jour**

126 Il vous incombe de tenir votre documentation et vos notifications à jour. Chaque fois qu'un changement intervient dans vos procédures qui a une incidence sur le contenu de la notification ou de la déclaration de confidentialité ou présente un intérêt sous l'angle de la protection des données, informez-en votre délégué à la protection des données. Il s'agit d'un élément important du processus d'obligation de rendre des comptes.

3.8. Mesures de sécurité techniques et organisationnelles

3.8.1. Gérez les risques liés à vos informations

R22: **Mettez en place un processus de gestion des risques correctement documenté pour sécuriser les informations**

127 Votre organisation doit mettre en place les mesures techniques et organisationnelles appropriées afin de garantir la sécurité d'utilisation des réseaux de communication électronique et des équipements terminaux (sécurité des systèmes et des données à caractère personnel), en collaboration avec les fournisseurs de services ou de réseaux si nécessaire. Conformément à l'article 22 du règlement, ces mesures devraient assurer un niveau de sécurité approprié au regard des risques présentés pour toutes les informations, compte tenu des solutions techniques disponibles et des coûts liés à leur mise en œuvre.

128 Cela signifie qu'il faut mettre en œuvre un **processus de gestion des risques liés aux informations** conformément aux principes établis en matière de bonnes pratiques (par exemple la série de normes ISO/CEI 27000). La première étape consiste en une évaluation des risques, qui devrait inclure une analyse de l'utilisation des ressources de communication électronique. Cette évaluation vous aidera à déterminer les principaux risques de sécurité et servira de base pour sélectionner les contrôles appropriés à mettre en place afin de réduire les risques à un niveau acceptable pour la gestion. Le processus de gestion des risques doit comporter un réexamen périodique de l'évaluation des risques et de l'adéquation des garanties et contrôles.

129 Vous devez documenter de façon appropriée le processus de gestion des risques liés à l'information, conformément aux normes établies pour cette procédure, et **communiquer** celui-ci en tant que politique de l'institution. Ce processus doit également être revu régulièrement afin de garantir qu'il conserve son efficacité et reste conforme aux objectifs opérationnels, qu'ils soient nouveaux ou modifiés.

130 Le processus (en particulier l'analyse des risques de sécurité) ne devrait **pas uniquement impliquer le personnel chargé des questions de sécurité** au sein de l'institution européenne concernée. L'**analyse doit prendre en compte l'incidence sur tous les domaines de l'organisation**, de sorte qu'un large éventail de représentants (RH, délégué à la protection des données, coordinateur de la protection des données, activités de base) doivent également être associés aux discussions.

131 Vous devriez clairement communiquer les résultats du processus de gestion des risques liés à l'information et les risques de sécurité existants à toutes les personnes concernées ou potentiellement concernées; l'encadrement et d'autres acteurs pourraient bénéficier d'une communication plus détaillée.

3.8.2. Externalisation de services

R23: **Prévoyez des clauses en matière de protection des données dans les contrats conclus avec les prestataires de services extérieurs**

132 Il est possible que les institutions européennes souhaitent sous-traiter certaines fonctions liées au traitement des données des communications électroniques à des prestataires extérieurs. Par exemple, votre organisation pourrait faire appel à des sociétés extérieures pour assurer la surveillance de la sécurité, la gestion des antivirus, la gestion du courrier électronique ou l'établissement de statistiques. Dans ce cas, des précautions appropriées doivent être prises. En particulier:

a. il convient que votre institution fasse preuve d'un grand soin dans le choix d'un sous-traitant qui offre des garanties suffisantes quant aux mesures de sécurité techniques et organisationnelles requises au titre du règlement: il incombe à l'**institution de veiller au respect** de ces mesures **par le sous-traitant**;

b. la relation entre l'institution européenne et le sous-traitant doit être **formalisée par un contrat ou un acte juridique** qui lie le sous-traitant au responsable du traitement. Ce document doit stipuler que:

   i. le sous-traitant n'agit que **sur instruction** de votre organisation;

   ii. les **obligations en matière de confidentialité et de sécurité** énoncées dans le règlement incombent également au sous-traitant (à moins que des obligations similaires ne s'appliquent déjà à celui-ci en vertu de la législation nationale mettant en œuvre la directive 95/46/CE). Pour les contractants situés en dehors de l'Union, des garanties adéquates doivent être assurées. Voir également le document exposant la position du CEPD sur le transfert de données à caractère personnel à des pays tiers et des organisations internationales par les institutions et organes de l'Union, en particulier les pages 18 à 21.

R24: **Surveillez les contractants pour veiller à ce qu'ils mettent correctement en œuvre les clauses prévues par leurs contrats**

133 Le règlement s'applique également à tout service externalisé, et il incombe à l'institution de veiller à ce que les sociétés extérieures suivent les principes qui y sont énoncés et mettent en œuvre les garanties appropriées, par exemple demander au personnel du contractant de signer des déclarations de confidentialité similaires à celles qui ont été signées par le personnel de votre propre organisation.

ANNEXE 1: RÉSUMÉ DES PRINCIPES RÉGISSANT LA PROTECTION DES DONNÉES

La liste ci-dessous donne un aperçu rapide des principes généralement reconnus en matière de protection des données. Vous trouverez l'ensemble ou la plupart d'entre eux dans les règles régissant la protection des données dans l'Union. Il vous revient, en tant que responsable du traitement, de les suivre et de pouvoir démontrer que vous le faites. Ils ne remplacent pas les conseils fournis dans les présentes lignes directrices, mais expliquent la philosophie qui sous-tend ceux-ci.

1. **Les données à caractère personnel doivent être traitées loyalement et licitement.**
   Vous devez vous assurer que vous disposez d'un motif licite pour traiter des données à caractère personnel. Ce peut être le cas, par exemple, si le traitement est nécessaire à l'accomplissement des tâches qui sont conférées à votre institution par la loi (y compris les activités administratives internes nécessaires). Par traitement loyal, on entend le fait de dire aux gens ce qu'il adviendra de leurs données et de s'en tenir à ce qui a été dit.

2. **Les données à caractère personnel doivent être collectées uniquement pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.**
   Déterminez explicitement pourquoi et comment vous traitez des données à caractère personnel. Ne les utilisez pas d'une manière incompatible avec cette finalité initiale.

3. **Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités poursuivies.**
   Réfléchissez aux données dont vous avez besoin pour les finalités que vous avez déterminées et traitez ces catégories de données exclusivement.

4. **Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour.**
   Veillez à ce que les données que vous traitez soient exactes, des données inexactes pouvant vous amener à prendre de mauvaises décisions. Le cas échéant, veillez à ce que les données soient mises à jour.

5. **Accordez des droits d'accès et de rectification**
   Les intéressés ont le droit d'accéder aux données à caractère personnel les concernant traitées par votre institution et de faire rectifier les données inexactes. Veillez à ce qu'ils puissent facilement exercer ces droits. Cela peut également vous aider à garantir que les données sont exactes et mises à jour.

6. **Les données à caractère personnel traitées ne doivent pas être conservées plus longtemps que nécessaire.**
   Réfléchissez à la durée pendant laquelle vous devez conserver les données et conservez-les ensuite pendant cette durée, mais pas au-delà.

7. **Veillez à la sécurité des données personnelles**
   Procédez à une évaluation des risques et prenez les mesures de sécurité appropriées en tenant compte de l'état de l'art, des risques liés au traitement et du coût de la mise en œuvre.

8. **Règles en matière de transferts**

Assurez-vous de suivre les règles spécifiques en matière de transfert de données à caractère personnel à des tiers, en particulier en cas de transfert en dehors de l'Union.