# Lignes directrices concernant le traitement de données à caractère personnel en matière de congé et d'horaire flexible

CEPD 2012-0158

Les présentes lignes directrices («**Lignes directrices**») sont publiées par le Contrôleur européen de la protection des données ("**CEPD**") dans l'exercice des pouvoirs qui lui sont conférés par l'article 41, paragraphe 2, et l'article 46, point d), du *règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données* («**le règlement**»).

Le contenu des présentes lignes directrices est basé sur les avis existants du CEPD en matière de congé et de système de gestion du temps (Flexitime), et plus précisément sur plusieurs avis concernant les opérations de traitement de données y afférentes par plusieurs institutions et organes de l'UE (voir annexe).

Les présentes lignes directrices portent sur le traitement de données à caractère personnel dans le cadre de la gestion de tous les droits relatifs aux congés maladie, congés annuels et, d'une manière générale, à tous les congés spéciaux[1] et conditions de travail y afférentes des fonctionnaires, agents temporaires (AT), agents contractuels (AC) et experts nationaux détachés (END). Les présentes lignes directrices incluent également une analyse des opérations de traitement Flexitime[2]. Elles couvrent le traitement de ces données par les services administratifs des institutions et organes de l'UE. Elles ne concernent dès lors pas le traitement correspondant des données par les services médicaux; ce type de traitement étant couvert par les lignes directrices du CEPD concernant le traitement des données

[1] Les congés couvrent les congés annuels, les congés maladie et les congés spéciaux suivants (décrits à l'annexe V du statut): adoption d'un enfant, adoption d'un enfant handicapé, déménagement, consultation en dehors du travail (plus de 65 km), citation à comparaître, décès des beaux-parents, décès d'un proche, décès du conjoint, décès de l'épouse pendant le congé de maternité, décès d'un frère/d'une sœur, décès d'un enfant, élections, examens/concours, cures de santé, absence irrégulière (exclusivement réservé au Bureau des congés), mariage, mariage d'un enfant, maternité, obligations militaires, autre raison, activités extérieures (article 12b), maladie grave des beaux-parents, maladie grave d'un ascendant, maladie grave du conjoint, maladie grave d'un enfant, formation, maladie très grave d'un enfant.

[2] L'objectif de toute politique d'horaire flexible est de rendre les méthodes de travail plus flexibles afin de faciliter la conciliation des obligations de la vie privée et de la vie professionnelle. Toute politique d'horaire flexible est conçue afin de permettre aux membres du personnel de parvenir à un meilleur équilibre entre leur vie privée et leur vie professionnelle dans le cadre d'un système juste et transparent visant à promouvoir l'égalité des chances. Le système Flexitime peut aussi être conçu pour permettre à l'institution de gérer plus efficacement la présence du personnel selon les exigences relatives au travail et d'améliorer la gestion des ressources humaines et budgétaires, y compris les heures supplémentaires.

relatives à la santé sur le lieu de travail par les institutions et organes de l'UE (anciennement communautaires)[3].

L'objectif principal des présentes lignes directrices est de donner des orientations à l'ensemble des organes et institutions de l'UE[4] pour le traitement des données à caractère personnel par leurs services administratifs, dans le cadre des procédures relatives aux congés et aux horaires flexibles. À cet égard, les présentes lignes directrices servent aussi à aider les délégués à la protection des données (DPD) et les responsables du traitement des données à notifier les traitements de données relatives aux congés et/ou aux horaires flexibles au CEPD en vue du contrôle préalable, le cas échéant.

La structure des présentes lignes directrices suit étroitement celle du formulaire de notification en vue du contrôle préalable. Le réseau des DPD a été consulté sur le projet de lignes directrices le 29 septembre 2012.

## 1. CONTRÔLES PRÉALABLES

L'article 27, paragraphe 1, du règlement prévoit que tous «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 sont **soumis au contrôle préalable du CEPD».** Les contrôles préalables servent à déterminer si un traitement de données prévu par une administration européenne est conforme au règlement, ou si le système doit être amélioré du point de vue de la protection des données.

### 1.1 Congés

- Le traitement de données relatives aux congés est susceptible d'impliquer le traitement de données relatives à la santé (par exemple, congé médical, congé de maternité et certains autres types de congés spéciaux) et relève dès lors de l'**article 27, paragraphe 2, point a)**, du règlement qui exige le contrôle préalable par le CEPD des «traitements de données relatives à la santé».

[3] Lignes directrices concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes communautaires: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_FR.pdf.
Bien que des liens existent entre ces deux documents, il convient de noter que les lignes directrices concernant les données médicales se réfèrent principalement au traitement des données médicales dans le cadre de l'examen médical d'embauche et de l'examen médical annuel et qu'une référence n'est faite aux congés que lorsque des données relatives à la santé sont traitées. Les lignes directrices en matière de congé et de flexitime sont, en revanche, axées sur toutes les catégories de congé et ne se limitent pas au traitement des données relatives à la santé. Ces lignes directrices doivent dès lors être considérées comme étant complémentaires, mais différentes les unes des autres.

[4] Il convient de noter que certaines institutions et certains organes de l'UE (à savoir, la Banque centrale européenne, la Banque européenne d'investissement) ne sont pas soumis au statut des fonctionnaires de l'UE ni au régime applicable aux autres agents, dans la mesure où ils disposent de leurs propres cadres en matière de droit du travail et de droit de la sécurité sociale, cadres qui, s'ils sont similaires en ce qui concerne le concept de statut de la fonction publique, présentent également des différences. Les éléments qui diffèrent sont soulignés dans les présentes lignes directrices, le cas échéant.

En ce qui concerne le concept de données relatives à la santé, le CEPD l'a défini dans ses lignes directrices concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes de l'UE[5]:

> «*Les données relatives à la santé désignent le plus souvent des données à caractère personnel présentant un lien avec l'état de santé d'une personne. Elles englobent normalement les données médicales (orientation d'un malade par un généraliste vers un spécialiste et prescriptions médicales, rapports d'examens médicaux, tests de laboratoire, radiographies, etc.), ainsi que les données administratives et financières relatives à la santé (calendrier des rendez-vous médicaux, factures de prestation de services de santé, indication du nombre de jours de congé de maladie, gestion des congés maladie, etc.)*».

Dès lors, même si les informations médicales sont conservées séparément des informations administratives, dans le cas de l'enregistrement des congés, le CEPD considère que les données à caractère personnel relatives à la santé sont néanmoins traitées. Les traitements y afférents doivent donc être contrôlés au préalable par le CEPD.

- Dans certains autres cas, lorsque des données concernant la présence sur le lieu de travail et les congés sont traitées pour évaluer le comportement d'un fonctionnaire, le contrôle préalable est exigé en vertu de l'**article 27, paragraphe 2, point b),** du règlement. Ceci vaut en particulier lorsque le traitement de données relatives aux congés permet d'évaluer le comportement des membres du personnel, y compris l'utilisation de ces données dans une évaluation annuelle et/ou une procédure de promotion. Dans un tel cas, le CEPD doit non seulement analyser les opérations de traitement si l'évaluation réalisée est explicitement prévue dans le cadre de la procédure, mais aussi si, eu égard à l'ensemble des éléments, il apparaît que le traitement est «destiné» à l'évaluation.

| |
|---|
| Par exemple, le CEPD évaluerait également une procédure relative aux congés qui ne prévoit aucune forme d'évaluation mais dont l'évaluation peut être déduite des autres éléments de la procédure (rapport ayant des conséquences sur le rapport annuel d'évaluation, la procédure de promotion, etc. ...). |

- Enfin, le traitement peut être couvert par l'**article 27, paragraphe 2, point d),** du règlement. C'est le cas des traitements caractérisés par une procédure de suivi administratif des absences injustifiées dues à des maladies, suivi qui engendre une réduction du droit aux congés et/ou une retenue sur salaire, à savoir «*les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat*».

[5] Voir le point intitulé «Concepts» des «Lignes directrices concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes communautaires», adoptées en septembre 2009, disponibles sur le site Internet du CEPD.

1.2 Flexitime

L'objectif initial du système Flexitime est de faciliter la conciliation des obligations de la vie privée et de la vie professionnelle des membres du personnel des institutions/organes de l'UE. À cette fin, les institutions/organes de l'UE peuvent autoriser leur personnel à répartir de manière inégale les 37½ heures hebdomadaires sur les cinq jours ouvrés, tout en respectant pleinement les dispositions du statut des fonctionnaires et les intérêts du service. En outre, et dans certaines limites, les crédits-temps accumulés peuvent être récupérés sous différentes formes (par heure, demi-journées ou journées complètes).

Ce faisant, les institutions/organes de l'UE souhaitent accroître la motivation des membres de leur personnel tout en les impliquant davantage dans l'organisation de leur temps de travail.

En principe, un système Flexitime n'est pas soumis au contrôle préalable [6] si:

- il vise l'utilisation efficace des ressources humaines (planification et répartition des ressources) et des ressources budgétaires et s'il ne concerne pas explicitement l'évaluation des membres du personnel, leur comportement, leur rendement, ou si
- les données relatives aux horaires flexibles ne sont pas traitées dans la procédure d'évaluation des membres du personnel et si la structure du système n'implique aucun *risque* clair d'utilisation à des fins d'évaluation.

En outre, si les services des ressources humaines souhaitent utiliser les données relatives aux horaires flexibles à d'autres fins (identification d'une charge de travail excessive, évaluation), ils doivent clairement préciser qu'il s'agit d'un objectif spécifique du traitement. Par ailleurs, étant donné l'objectif initial du système Flexitime, le CEPD considère également que, eu égard aux données normalement traitées par un tel système (à savoir, rapport individuel du temps passé au travail), les services des ressources humaines ne peuvent fonder une évaluation sur ces seules données ou mettre en évidence l'existence d'une charge excessive de travail d'un membre du personnel en se fondant sur ces seules données.

Les paragraphes suivants examinent les cas dans lesquels l'article 27 du règlement s'applique et ceux dans lesquels un contrôle préalable est exigé.

**-Article 27, paragraphe 1**: en principe, lorsqu'un système d'identification par radiofréquence (RFID) est utilisé dans des domaines liés aux ressources humaines (comme un badge pour l'application Flexitime), une telle application implique le traitement de données à caractère personnel. Même si la puce ne contient qu'un numéro d'identification, ce numéro ainsi que toutes les autres données qui lui sont liées, sont des données à caractère personnel au sens défini de la directive 95/46 et du

[6] Le CEPD a également estimé, dans le dossier 2007-0063, que les DG de la Commission ainsi que les agences qui suivent les prescriptions de la DG Ressources humaines (précédemment ADMIN) relatives à Flexitime sont couvertes par sa notification générale, tout en conservant une responsabilité locale. Ce n'est que si une DG ou une agence devait utiliser un système différent de celui de la notification générale de la Commission qu'elle devrait notifier séparément les aspects de son système qui diffèrent de ceux établis par la DG Ressources humaines et qui auraient des conséquences pour la protection des données.

règlement (CE) n° 45/2001, dans la mesure où ce numéro ne concerne que la personne concernée, à savoir l'employé qui détient le badge[7].

Lors de la mise en œuvre d'une application Flexitime utilisant la technologie RFID, le responsable du traitement des données devrait tenir compte des meilleures pratiques existantes[8], y compris la réalisation des évaluations d'impact sur la protection des données[9] afin d'évaluer les risques que l'application peut présenter pour la vie privée et devrait prendre les mesures techniques et organisationnelles appropriées pour limiter les risques identifiés, en appliquant le principe du respect de la vie privée dès la conception. Lorsqu'il ressort de l'évaluation d'impact qu'il existe des risques spécifiques pour la personne concernée, le traitement doit être notifié au CEPD en vue d'un contrôle préalable.

- **Article 27, paragraphe 2, point a)**: si le système Flexitime dans son ensemble couvre également l'enregistrement des congés maladie, l'article 27, paragraphe 2, point a), s'applique étant donné que les congés maladie sont susceptibles de révéler l'état de santé d'une personne concernée. Toutefois, la nécessité d'un contrôle préalable, au titre de l'article 27, paragraphe 2, point a) du règlement, n'est justifiée que si le traitement des données concerné implique le traitement de données relatives à la santé de manière régulière, et non uniquement de manière purement occasionnelle ou accidentelle. Si le traitement ne révèle, par exemple, que la présence du mot «congé» sur le relevé des heures de travail, cela n'est pas considéré comme étant suffisant pour justifier un contrôle préalable.

- **Article 27, paragraphe 2, point b):** dans certains cas, les données à caractère personnel traitées par le système Flexitime peuvent relever du champ d'application de l'article 27, paragraphe 2, point b) lorsque les présences sur le lieu de travail sont utilisées pour évaluer le comportement d'un fonctionnaire. Cela vaut en particulier lorsque le traitement de données relatives aux heures de travail et aux absences par le système Flexitime est censé rendre possible l'évaluation du comportement d'un fonctionnaire, y compris son utilisation aux fins de l'évaluation annuelle et/ou de la procédure de promotion ou s'il est prévu que les données rassemblées peuvent

[7] Voir PC 2007-0218 sur la «mise en œuvre du Flexitime spécifique à la DG INFSO» et 2008-697 sur «la mise en œuvre de Flexitime à l'ETF».

[8] Des lignes directrices relatives à des questions de protection des données liées à la technologie RFID ont été formulées dans plusieurs avis du CEPD et du Groupe de travail «Article 29», tels que le «Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)» rédigé par le Groupe «Article 29», 19.1.2005, disponible sur le site Internet Europa; l'avis du CEPD sur la communication de la Commission relative à la technologie RFID, 2007; l'avis du CEPD sur le respect de la vie privée à l'ère numérique.

[9] Par exemple, la recommandation de la Commission C(2009) 3200 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radio-fréquence indique au point 5 que les exploitants d'applications RFID devraient:

a) réaliser une évaluation des incidences de la mise en œuvre de l'application sur la protection des données à caractère personnel et le respect de la vie privée;
b) prendre les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel et le respect de la vie privée;
c) désigner une personne ou un groupe de personnes chargées de réexaminer les évaluations et l'adéquation constante des mesures techniques et organisationnelles pour assurer la protection des données à caractère personnel et le respect de la vie privée;
d) mettre l'évaluation à la disposition de l'autorité compétente au moins six semaines avant le déploiement de l'application.

également être utilisées afin d'évaluer le comportement d'un membre du personnel en cas de suspicion de mauvais comportement de ce dernier. Le CEPD souligne que cela doit s'appliquer que l'objectif de l'évaluation du personnel soit *explicite* ou *implicite* (l'existence d'un objectif implicite peut être déduite des caractéristiques objectives du système, par exemple, l'existence de rapports individuels, de périodes de conservation, etc.).

- **Article 27, paragraphe 2, point c):** il est possible que le traitement des données relatif au système Flexitime relève aussi de l'article 27, paragraphe 2, point c). Cet article prévoit le contrôle préalable des «*traitements permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées pour des finalités différentes*». Cette disposition vise avant tout à éviter que des données collectées à des fins différentes ne soient interconnectées pour des finalités différentes. En interconnectant des données Flexitime avec un autre système (par exemple, un système de contrôle d'accès), des interconnexions peuvent être créées et ces interconnexions peuvent ne pas être prévues par la législation nationale ou européenne. Dans un tel cas, l'article 27, paragraphe 2, point c) s'applique. C'est l'interconnexion des traitements qui serait analysée dans une telle situation et non simplement le traitement des données Flexitime.

Si une telle interconnexion est réalisée en vue de la vérification des pointages Flexitime par rapport aux données sur le contrôle physique des accès, le CEPD a déjà indiqué que le caractère nécessaire et proportionnel d'un tel traitement est très discutable et qu'il considère une telle interconnexion comme étant excessive. De manière générale, le CEPD n'est pas favorable aux systèmes qui viseraient à combiner le traitement de données à caractère personnel dans le cadre du système Flexitime et le traitement de données à caractère personnel dans le cadre de contrôles d'accès à des fins de conformité/vérification. Le CEPD considère que les institutions et les organes disposent d'autres moyens pour identifier les membres du personnel qui ne respectent pas les règles en vigueur.

Enfin, le CEPD attire l'attention des institutions et des organes de l'UE sur le fait qu'il n'est pas non plus favorable à des systèmes qui autoriseraient le traitement de données à caractère personnel tant à des fins relatives aux horaires flexibles qu'à des fins de contrôle d'accès. En effet, ces opérations de traitement sont prévues par les institutions et organes de l'UE dans deux buts distincts (horaires variables d'une part, et contrôle d'accès d'autre part); l'accès aux données est limité aux personnes responsables au sein de l'institution/organe (la plupart du temps, le personnel du service des ressources humaines pour le système Flexitime, et les responsables locaux de la sécurité pour les données de contrôle d'accès); et les périodes de conservation des données applicables à chaque traitement sont différentes.

## 2. LICÉITÉ DU TRAITEMENT

Dans le cadre des congés et des horaires flexibles, la licéité du traitement doit être considérée, dans la plupart des cas, à la lumière de l'article 5, point a) du règlement: «*Le traitement de données à caractère personnel ne peut être effectué que si le traitement 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 ou relevant de l'exercice légitime de l'autorité publique dont est investi l'institution ou l'organe communautaire ou le tiers auquel les données sont communiquées*». À cet égard, le considérant 27 du règlement indique également que «*[l]e traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes*».

La base juridique du traitement des données à caractère personnel se trouve dans le statut des fonctionnaires (SF).

Les congés sont, de manière générale, traités dans le cadre du chapitre 2 du titre IV: «Conditions de travail du fonctionnaire» du statut des fonctionnaires (articles 57-60), qui s'applique par analogie aux autres agents de l'Union européenne, définis aux titres III et IV du statut des fonctionnaires:

- les congés annuels (article 57 SF), congés spéciaux (annexe V SF), congés de maternité (article 58 SFR), congés maladie/congés familiaux (article 59 SF), congés de convenance personnelle et congés non payés (articles 15, 37 et 40 SF) forment la base juridique de ces opérations de traitement;

- par ailleurs, les articles 11, 16 to 18, 58, 81 et 91 du *Régime applicable aux autres agents des Communautés européennes* prévoient le droit aux congés pour les agents non couverts par le statut des fonctionnaires, mais qui sont néanmoins employés en tant qu'agents temporaires ou agents contractuels;

- enfin, il est possible que des dispositions d'exécution des institutions et organes adoptées sur la base de l'article 110 du statut des fonctionnaires fournissent une base juridique complémentaire à la lumière de l'article 5, point a) du règlement.

Le CEPD note que le traitement des données à caractère personnel relatives aux congés est considéré comme étant nécessaire pour permettre aux institutions et organes de remplir leurs obligations envers le personnel, conformément aux règles susmentionnées. Dès lors, le traitement des données à caractère personnel effectué dans ce contexte sera considéré comme étant licite, conformément à l'article 5, point a) du règlement.

- L'article 55 du SF constitue la base juridique du traitement des données relatives aux horaires flexibles, compris en tant que régime de travail permettant au personnel de concilier vie professionnelle et vie privée. Ce régime de travail doit également être mentionné dans une décision sur le système d'horaires flexibles adoptée par l'institution/organe concerné. Si une institution ou un organe de l'UE souhaite adopter une procédure visant une autre finalité ou d'autres finalités, le CEPD considère que l'article 55 ne constitue pas une base juridique suffisante et une autre base juridique doit être adoptée afin de refléter cette différence de finalité.

## 3. TRAITEMENT DE CATÉGORIES SPÉCIALES DE DONNÉES

En vertu de l'article 10 du règlement, le traitement de certaines données sensibles est interdit, sauf dans certaines circonstances prédéfinies.

En vertu de l'article 10, paragraphe 1, du règlement, «*[l]e traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle sont interdits*».

L'article 10, paragraphe 2, du règlement contient une liste des exceptions levant l'interdiction générale du traitement de ces données.

- En particulier, en vertu de l'article 10, paragraphe 2, point b), «*le traitement est nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités ou, si cela s'avère nécessaire, dans la mesure où il est accepté par le contrôleur européen de la protection des données, moyennant des garanties adéquates*».

Dans la plupart des cas, dans le cadre des congés, le traitement de certaines données relatives à la santé est considéré comme étant nécessaire afin de respecter les obligations légales conformément aux articles 59 et 60, et à l'annexe V du statut des fonctionnaires et aux articles 16, 58 et 91 du régime applicable aux autres agents des Communautés européennes. Le traitement est dès lors jugé nécessaire pour respecter les droits et obligations du responsable du traitement dans ce domaine.

Cette justification peut s'appliquer dans les cas suivants:

- le traitement de données à caractère personnel relatives à la santé dans le cadre des congés maladie est susceptible de révéler des éléments concernant l'état de santé de la personne concernée. En outre, lorsqu'un certificat médical est fourni, la spécialisation médicale du médecin peut potentiellement fournir des informations supplémentaires sur la santé de la personne concernée.

> Normalement, les données relatives à la spécialisation du médecin ne doivent être envoyées qu'au service médical. Cependant, en cas de rendez-vous médical pendant les heures de travail, la personne concernée doit généralement fournir à la personne chargée de la gestion des congés dans son institution/organe un certificat de présence et la spécialisation du médecin est susceptible d'apparaître sur ce certificat. Cette situation est couverte par l'article 10, paragraphe 2, point b).

- le traitement de données à caractère personnel relatives à la santé dans le cadre de congés en relation, par exemple, avec l'adoption d'un enfant handicapé, des cures de santé, la maladie grave du conjoint, et à d'autres types de congés spéciaux. En outre, en cas de congé parental et de congé familial, un traitement supplémentaire des données relatives à la santé a lieu. Des données

pouvant révéler l'orientation sexuelle d'un membre du personnel et de son partenaire sont aussi traitées lorsqu'un membre du personnel demande un congé pour s'occuper de son partenaire ou en cas de mariage homosexuel;

- le traitement de données à caractère personnel relatives à la santé dans le cadre d'une visite médicale aux fins du contrôle et de la gestion des congés en cas d'absences. Le statut des fonctionnaires, le régime applicable ainsi que les dispositions d'exécution respectives exigent le traitement des données relatives à la santé dans de tels cas; ces données relèvent de l'article 10, paragraphe 2, point b).

## 4. QUALITÉ DES DONNÉES

En vertu de l'article 4, paragraphe 1, points a), c) et d) du règlement, les données à caractère personnel doivent être traitées loyalement et licitement, être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, et être exactes.

**Pertinence et proportionnalité**: en vertu de l'article 4, paragraphe 1, point c) du règlement, les données doivent être «*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*».

Le CEPD considère qu'il est opportun qu'aucune donnée médicale ne soit contenue dans l'attestation pouvant être envoyée par le service médical aux ressources humaines. Cette attestation ne devrait contenir que des données administratives.

Comme il l'a déjà souligné dans les lignes directrices concernant les données relatives à la santé, le CEPD a connaissance de ce que, dans certaines agences, aucun service médical n'a été mis en place et que celles-ci délèguent le traitement de toutes les données médicales au service médical de la Commission européenne ou à un fournisseur de services externe (c'est-à-dire à un médecin extérieur). Dans ce cas, le CEDP renvoie à ses recommandations formulées dans les lignes directrices concernant les données relatives à la santé (paragraphe 8).

En outre, en règle générale, seules les informations nécessaires devraient être traitées.

Par exemple, si quelqu'un demande un congé spécial afin de participer à un concours, de nombreux documents sont requis: le formulaire d'inscription, la convocation à l'examen et la preuve de la présence le jour du concours. Le CEPD considère que, à la lumière du principe de qualité des données, la seule communication de la convocation et de l'attestation de présence doit suffire pour ce type de congé. Cette position est conforme, par exemple, à la décision de la Commission européenne du 5 novembre 2010 sur la mise en œuvre de dispositions

Les données à caractères personnel des personnes à charge ou des proches (comme le handicap ou la maladie de l'enfant, par exemple) peuvent donner lieu à un congé ou à un régime du temps de travail différent (temps partiel). Le CEPD souligne, à titre de

ligne directrice générale, que seules des obligations juridiques spécifiques peuvent entraîner le traitement, dans le système des congés/horaires flexibles, de données à caractère personnel et de données sensibles concernant les proches, et ce uniquement aux fins de la gestion des heures de travail/des congés dans la mesure où cela est nécessaire à cette fin.

En cas d'utilisation d'un système d'horaire flexible combiné à un système de badge, outre les données d'identification, le CEPD a considéré qu'il est opportun de collecter les numéros d'identification des membres du personnel ainsi que leurs heures d'entrée et de sortie. Le CEPD souligne en outre que, dans tout système d'horaire flexible volontaire, les données relatives aux heures d'entrée et de sortie des membres du personnel qui ne souhaitent pas participer au programme d'horaire flexible ne devraient pas être traitées.

Par ailleurs, pour ce qui est de l'exactitude des données, comme cela a déjà été expliqué ci-dessus, l'objectif initial du système est de faciliter la conciliation entre vie professionnelle et vie privée des membres du personnel et ce système ne vise pas spécifiquement à détecter les fraudes. Si le CEPD reconnaît l'existence d'un contrôle normal de l'exactitude des données relatives aux horaires flexibles introduites par le personnel, contrôle exercé par le supérieur, cela ne doit pas engendrer des situations dans lesquelles les membres du personnel devraient, par exemple, signer un registre de présence lorsque le système d'horaire flexible qui est utilisé par l'institution/organe de l'UE permet déjà de vérifier l'exactitude des données en autorisant le supérieur immédiat et la personne concernée à accéder aux données Flexitime (Sysper2, par exemple). Une telle procédure devrait être suffisante pour garantir l'exactitude des données.

**Exactitude:** l'article 4, paragraphe 1, point d) du règlement prévoit que les données doivent être «*exactes et, si nécessaire, mises à jour*». Cet article indique également que *«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»*.

Le CEPD souligne également que si la personne concernée adresse une demande relative à l'exactitude de ses données, cette demande doit être enregistrée. La personne concernée doit également bénéficier du droit d'accès et du droit de rectification en ce qui concerne les données (administratives), afin de les rendre le plus exactes et complètes possible.

En ce qui concerne les systèmes Flexitime, le CEPD souligne que, pour que les données soient exactes et à jour, le système doit en général être conçu de manière à garantir l'exactitude et la mise à jour des données. Il convient en outre, afin de garantir l'exactitude des données, de respecter le droit d'accès de la personne concernée aux données la concernant à des fins de vérification ainsi que son droit de rectification.

**Traitement loyal et licite:** les données doivent être «*traitées loyalement et licitement*» (article 4, paragraphe 1, point a) du règlement). Le caractère licite du traitement doit être assuré conformément à la licéité examinée au point 2 ci-dessus. Le

traitement loyal signifie que des informations pertinentes et complètes sont transmises aux personnes concernées (ce point est examiné ci-dessous au point «Informations»).

## 5. CONSERVATION DES DONNÉES

En vertu de l'article 4, paragraphe 1, point e) du règlement, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle **nécessaire** à la réalisation des **finalités** pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. La conservation de données au-delà de la période précitée à des fins historiques, statistiques ou scientifiques n'est possible que sous une forme qui les rend anonymes. Par conséquent, le CEPD estime qu'il n'existe pas de justification permettant de conserver les données indéfiniment, vu la finalité initiale de leur collecte.

En outre, en règle générale, en ce qui concerne la suppression des enregistrements à carcatère financier, sur la base de l'article 49 des modalités d'exécution du règlement financier «*[l]es données à caractère personnel contenues dans les pièces justificatives sont supprimées si possible lorsqu'elles ne sont pas nécessaires aux fins de la décharge budgétaire, du contrôle et de l'audit*».

Le CEPD insiste sur le fait que des périodes de conservation doivent être clairement fixées pour les différents types d'absences et que ces périodes s'appliquent tant aux données/pièces justificatives en ligne qu'aux données/pièces justificatives sur papier.

Les périodes de conservation dépendent du type de congé et varient selon les finalités pour lesquelles les données ont été collectées et traitées. En raison des spécificités liées aux différents types de congés, les sections suivantes examineront les différents types de données collectées et traitées pour le type de congé concerné à la lumière des lignes directrices émises par le CEPD dans ses avis.

### 5.1. CONGÉS MALADIE

Les contrôles des absences pour maladie visent à garantir que l'absence est justifiée.

En règle générale, le CEPD considère qu'une période de conservation d'au moins trois ans pour les données administratives relatives aux congés maladie peut être justifiée pour les ressources humaines par l'article 59, paragraphe 4, du statut des fonctionnaires. Cet article prévoit que l'autorité investie du pouvoir de nomination peut saisir la commission d'invalidité du cas du fonctionnaire dont les congés cumulés de maladie excèdent douze mois pendant une période de trois ans. Cependant, le CEPD accepte la proportionnalité d'une période de conservation supérieure à trois ans qui serait strictement requise[10]. Une période de conservation plus longue par les

[10] Voir, par exemple, les lignes directrices du CEPD concernant le traitement des données relatives à la santé sur le lieu de travail, page 12: «l'article 59, paragraphe 4, du statut des fonctionnaires pourrait légitimer une période de conservation de trois ans pour les données nécessaires afin de justifier une absence liée à la prise de congés de maladie. Une durée de conservation supérieure ne serait justifiée qu'en cas de litige ou de recours».

ressources humaines pourrait dès lors s'appliquer afin de couvrir des périodes pendant lesquelles un litige ou un recours est en cours[11].

5.2. CONGÉS ANNUELS

La conservation de données relatives aux jours de congé annuel peut être justifiée si les congés sont reportés d'une année sur l'autre. En outre, il est possible qu'une institution/un organe prenne en considération les autres congés pris par une personne au cours des années précédant immédiatement l'année concernée afin d'améliorer la gestion et la coordination. Dès lors, s'agissant d'une période de conservation raisonnable et en vue d'aligner la durée des différentes périodes de conservation, le CEPD accepte une période de conservation maximale de trois ans pour les congés annuels.

5.3. AUTRES CONGÉS

Il est opportun de conserver les données relatives aux temps partiels, aux congés parentaux et familiaux jusqu'à la fin de l'engagement au sein de l'institution concernée, voire au-delà, si certains droits de la personne concernée persistent ou en cas de recours en cours.

Par exemple, en ce qui concerne le congé familial, les données peuvent être conservées pendant toute la carrière de la personne aux fins de la détermination du moment auquel la durée totale du congé accordé atteint le maximum autorisé (article 42 ter, du statut des fonctionnaires).

Un autre exemple concerne le congé de convenance personnelle: les données sont conservées pendant toute la carrière de la personne afin de pouvoir calculer quand la totalité du congé accordé atteint le maximum autorisé de 15 ans (article 40, paragraphe 2, du statut des fonctionnaires.

Certains congés spéciaux, par exemple dans le cadre du crédit-temps, ont un effet sur le calcul de la pension et nécessitent de conserver les données pendant de plus longues périodes.

Les institutions et organes de l'UE peuvent également prévoir des règles concernant les compensations financières en matière de congé. Dans de tels cas, en ce qui concerne les paiements relatifs à des congés non pris lors de la cessation des fonctions ou en cas d'heures supplémentaires pouvant être compensées par du temps libre rémunéré (paiements compensatoires au lieu de congés), le CEPD estime qu'il est opportun de conserver les données pendant une durée maximale de sept ans. Cette période de conservation est conforme au régime de l'UE applicable à la destruction de dossiers à caractère financier. Dès lors, en vertu de l'article 49 des modalités

[11] La conservation des données médicales par les services médicaux est couverte par les lignes directrices concernant la santé sur le lieu de travail. Si, toutefois, une institution ou un organe souhaite conserver pendant une période plus longue des dossiers relatifs à des congés maladie qui pourraient être liés à des cas médicaux dans le cadre desquels les conséquences médicales de l'exposition prolongée à certaines substances n'apparaissent qu'après une assez longue période (comme cela peut être le cas pour l'amiante ou l'exposition aux rayonnements), cela doit être prévu spécifiquement dans la procédure prévue concernant les données relatives à la santé.

d’exécution du règlement financier, les pièces justificatives originales doivent être conservées pendant sept ans après la décharge budgétaire. Cependant, en vertu du même article 49, les données à caractère personnel contenues dans les pièces justificatives doivent être supprimées dès qu’elles ne sont plus nécessaires aux fins de la décharge budgétaire, du contrôle et de l’audit.

5.4. FLEXITIME

Les données sur l’horaire Flexitime des employés ne peuvent être conservées que pendant l’année calendrier en cours. Elles doivent être effacées une fois que les jours de congés annuels non utilisés ont été récupérés l’année suivante, et au plus tard à la fin du mois de mars de l’année suivante.

Cependant, lorsque le calcul des heures quotidiennes de travail est réalisé au niveau du chef d’unité/de secteur et se base sur des déclarations intermédiaires, les données brutes doivent être détruites une fois que l’évaluation mensuelle a été validée par le chef d’unité/de secteur, en tenant compte de la période pendant laquelle les membres du personnel peuvent introduire une réclamation. La période de conservation ne peut dès lors pas être supérieure à trois mois.

Si un système d’horaire flexible est mis en place en vue d’une utilisation en tant qu’outil éventuel permettant d’évaluer le personnel ou d’obtenir des indications sur la charge de travail, il devra non seulement respecter les conditions susmentionnées concernant la base juridique et la limitation de la finalité, mais la période de conservation devra également être adaptée à la finalité du traitement et être couverte par la base juridique pertinente.

Les données relatives aux horaires flexibles des membres du personnel qui quittent l’institution/l’organe ou de ceux qui ne souhaitent plus participer au programme Flexitime doivent être supprimées dans un délai d’un ou deux mois dans la mesure où aucun élément ne peut justifier leur conservation plus longtemps, en raison des droits des personnes concernées mentionnés dans les règles de l’institution/organe relatives au système Flexitime.

Si le système Flexitime fonctionne au moyen d’un système de badges électroniques, la plupart du temps les lecteurs du système Flexitime joueront le rôle de mémoire tampon pour les pointages avant le transfert des données vers le système des congés. Dans ce cas, considérant qu’il est nécessaire de conserver une piste d’audit de l’enregistrement des données, le CEPD accepte que toutes ces données soient conservées pendant une durée maximale de deux mois.

## 6. TRANSFERTS DE DONNÉES

Dans ses avis sur les aspects de la protection des données en matière de congés, le CEPD identifie trois types possibles de transferts: entre institutions ou organes de l’UE ou en leur sein (article 7 du règlement).

6.1. Transferts en vertu de l'article 7 du règlement

Les transferts entre institutions ou organes de l'UE ou en leur sein ne sont conformes à l'article 7, paragraphe 1, du règlement que si «*les **données** sont **nécessaires** à **l'exécution légitime** de missions relevant de la compétence du destinataire*» (gras ajouté).

La nécessité du transfert au titre de l'article 7 est interprétée en ce sens que l'institution, l'organe ou l'agence destinataire doit d'abord «*établir que le transfert était indispensable*» en vue de l'exécution légitime de missions[12]. En outre, le transfert de données à caractère personnel doit respecter l'article 4, paragraphe 1, point b), et l'article 6 du règlement. En effet, l'article 7 s'applique sans préjudice des articles 4, 5, 6 et 10. Dès lors, le transfert ne peut entraîner la modification des finalités pour lesquelles les données ont été collectées et traitées à l'origine. Si le transfert entraine toutefois un changement de finalité, cela doit être expressément prévu dans la législation et la personne concernée doit en être informée. Afin que le règlement soit pleinement respecté, seules les données pertinentes peuvent être transférées et, une fois transférées, elles ne peuvent être traitées qu'en vue des finalités pour lesquelles elles ont été transmises.

Dans le cadre des **congés**, les données sont communiquées à d'autres unités ou responsables chargés de la gestion du personnel (directeur si ce dernier agit en tant qu'autorité investie du pouvoir de nomination, par exemple). Le transfert est nécessaire pour gérer les tâches liées à l'emploi de ces unités. Ces transferts ne peuvent être requis que lorsqu'il convient de décider si une absence est justifiée ou non ou de tirer des conclusions administratives ou disciplinaires, mais pas dans tous les cas, lorsque l'intervention du supérieur hiérarchique ou du chef d'unité doit normalement suffire.

Les documents administratifs contenant des données relatives à la santé ne doivent être communiqués qu'aux destinataires qui ont besoin d'en connaître et sont liés par une obligation de secret professionnel équivalant à l'obligation de secret professionnel des médecins. Les informations concernant l'état de santé d'une personne qui ne sont pas nécessaires aux finalités pour lesquelles les données sont transmises doivent être effacées de ces documents.

Cela est encore plus pertinent dans le cadre du traitement de données sensibles comme les données relatives à la santé. Le CEPD confirme que seules les conclusions sur la question de savoir si un congé est justifié ou si un candidat est apte au travail peuvent être transférées aux départements susmentionnés[13].

Le transfert peut parfois avoir lieu vers le service juridique, le Tribunal de la fonction publique, le Médiateur européen ou le CEPD. Le CEPD considère que de tels transferts sont conformes à l'article 7 du règlement s'ils sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire.

[12] Arrêt du Tribunal de la fonction publique du 5 juillet 2011, dans l'affaire F - 46/09, V./Parlement européen, point 131.

[13] En ce qui concerne le transfert des factures médicales, le CEPD renvoie à ses Lignes directrices concernant le traitement des données relatives à la santé sur le lieu de travail par les institutions et organes communautaires (aujourd'hui de l'UE).

Enfin, en vertu de l'article 7, paragraphe 3, du règlement, il convient de rappeler à tous les destinataires des données de ne pas traiter les données reçues à d'autres fins que celles pour lesquelles elles leur ont été transmises.

En ce qui concerne le système Flexitime, les données ne doivent être transférées qu'au service compétent du responsable du traitement (à savoir, les ressources humaines). Le CEPD estime que le responsable (local) de la sécurité ne doit pas être destinataire des données provenant d'un système Flexitime. En effet, la situation régnant dans une application flexitime diffère de l'objectif de sécurité associé, par exemple, au numéro de la carte qui doit servir au contrôle de l'accès au bâtiment. Dans le cas de l'horaire flexible, l'accès au numéro «Flexitime» de la carte doit être limité aux personnes compétentes de l'institution/organe, dont le responsable local de la sécurité ne fait pas partie.

## 7. CHANGEMENT DE FINALITÉ/USAGE COMPATIBLE

En vertu de l'article 4, paragraphe 1, point b), du règlement, les données à caractère personnel doivent être «*collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [..]*». Tout changement de finalité doit être justifié.

Sans préjudice des articles 4, 5 et 10, l'article 6, paragraphe 1, prévoit que «*[l]es données à caractère personnel ne peuvent être traitées pour des finalités autres que celles pour lesquelles elles ont été collectées que si le changement de finalité est expressément autorisé par les règles internes de l'institution ou de l'organe communautaire*».

### Congés

Les données sont traitées aux fins de la gestion des congés des membres du personnel. Ces données peuvent aussi faire l'objet d'un traitement ultérieur dans le cadre de la procédure de mise en invalidité, conformément à l'article 59, paragraphe 4, du statut des fonctionnaires. À cet égard, le CEPD note que le traitement ultérieur peut être considéré comme étant compatible.

### Flexitime

La collecte des données relatives à l'horaire flexible a pour objectif d'enregistrer les heures travaillées. Tout changement de cette finalité doit dès lors être examiné à cet égard. Le cas de l'interconnexion des données Flexitime avec une autre base de données peut constituer un exemple de changement de finalité éventuel (article 27, paragraphe 2, point c).

- Par exemple, le CEPD s'est opposé à la possibilité de lier une base de données de contrôle d'accès à une base de données Flexitime. Pour le CEPD, la vérification des pointages Flexitime par rapport aux données sur le contrôle physique des accès ne peut être justifiée comme étant nécessaire que lorsqu'il existe des raisons de soupçonner qu'un membre du personnel enfreint les règles relatives à l'horaire

flexible. Cette vérification devrait alors être effectuée dans le cadre d'une enquête administrative et non sur une base automatique.

- Un autre changement de finalité possible concerne l'interconnexion entre un outil de gestion du personnel facilitant l'organisation du travail et Flexitime. Dans ce cas, le CEPD pourrait accepter le changement de finalité, mais il insisterait sur le fait que les règlements intérieurs couvrant tant le système Flexitime que l'outil de gestion doivent être modifiés pour y insérer une clause autorisant la réutilisation des pointages issus du système Flexitime dans le cadre de l''autre système. Cette modification devrait aussi être introduite dans les règles internes sur le système interconnecté, qui devraient être modifiées afin de citer le système Flexitime comme l'une de leurs sources de données.

Enfin, le CEPD souligne également le fait que si le système Flexitime ne doit pas être utilisé dans le cadre du processus d'évaluation, les données Flexitime ne peuvent être conservées par les chefs d'unité et leur secrétariat, étant donné que, si tel était le cas, les données pourraient être utilisées directement ou indirectement à des fins d'évaluation, ce qui constituerait de prime abord un cas de changement de finalité. Dès lors, lorsqu'un supérieur autorise un membre du personnel à travailler en suivant un horaire flexible, les données relatives à l'horaire flexible doivent être effacées par le supérieur.

## 8. DROITS DES PERSONNES CONCERNÉES

L'article 13 du règlement prévoit un droit d'accès – ainsi que les modalités pour l'exercer – à la demande des personnes concernées. L'article 14 prévoit un droit de rectification des données à caractère personnel inexactes ou incomplètes.

Toute procédure en matière de congés doit décrire la possibilité pour un membre du personnel d'accéder aux données à caractère personnel le concernant et mentionner la possibilité qu'il a de les rectifier.

Le droit d'**accès**, le droit de rectification et le droit d'opposition doivent être accordés comme suit: toutes les données à caractère personnel (congés/absences/travail à temps partiel/congé parental et familial/horaire flexible) doivent être accessibles par le titulaire de ces données (qui sont en réalité en partie fournies par ce dernier). Le membre du personnel peut dès lors les vérifier et, si nécessaire, les corriger directement ou demander qu'elles soient corrigées par un gestionnaire compétent (données relatives à l'identification) ou par son supérieur hiérarchique immédiat (souvent dans le cas d'un système Flexitime).

Pour la partie des données relatives aux aspects temporels (a priori fournies par le titulaire du poste), certaines de ces données doivent être validées et corrigées, le cas échéant, par un gestionnaire de congés ou par l'AIPN, surtout si elles influencent des droits financiers et/ou la durée d'attribution des droits de la personne qui a introduit les données (pour le congé parental la notion d'allocation majorée et/ou parent isolé).

Concernant l'utilisation d'un système **Flexitime** basé sur des technologies RFID, le CEPD s'est déjà félicité de la distinction opérée entre deux catégories de données traitées: les données relatives à l'identification et les données spécifiquement liées à l'horaire flexible.

- Les données relatives à l'identification sont liées au système de gestion administrative et peuvent, si nécessaire, être modifiées en suivant la procédure relative à ce système. On pourrait autoriser l'accès à ces données aux personnes concernées via un identifiant et un mot de passe, conformément aux mesures adoptées par l'institution/organe. Les personnes concernées (utilisateurs de l'application) pourraient accéder à leurs données, les vérifier et, si nécessaire, les corriger.

- En ce qui concerne les données liées à l'application Flexitime, les personnes concernées peuvent utiliser un module Flexitime (elles-mêmes ou par l'intermédiaire de leur supérieur hiérarchique) pour accéder à leurs données à caractère personnel, les vérifier et, si nécessaire, les corriger. Dès lors, si le supérieur hiérarchique accepte un accès individuel, les membres du personnel peuvent eux-mêmes corriger/compléter l'enregistrement des pointages au cours d'un certain laps de temps, en général entre une semaine et dix jours. Une fois cette période écoulée, ou si le supérieur hiérarchique a opté pour une approche centralisée, les membres du personnel doivent adresser les demandes visant à corriger/compléter les données qui les concernent à leur supérieur hiérarchique ou à un gestionnaire désigné.

En ce qui concerne les droits de **rectification et de verrouillage**, dans certains cas, le droit de rectifier des données est lié au droit de verrouiller des données, par exemple lorsque la personne concernée affirme qu'elles ne sont pas exactes. En vertu de l'article 14 du règlement, «*[l]a personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données à caractère personnel inexactes ou incomplètes*». Pendant la période nécessaire au responsable du traitement pour vérifier l'exactitude des données ces dernières doivent être verrouillées (à la demande de la personne concernée).

Étant donné que l'exercice du droit de rectification doit être accordé «sans délai», le droit de verrouillage des données doit aussi être accordé sans délai et doit même précéder le droit de rectification.

Toutefois, dans les rares cas d'utilisation d'un système de gestion (que ce soit pour les congés ou les horaires flexibles) qui n'inclut pas la possibilité de verrouiller les données de manière sélective, le verrouillage des données est susceptible de créer des problèmes pour l'ensemble du système. Dans de tels cas, le CEPD est favorable à une procédure spécifique: chaque fois que le verrouillage des données est demandé par la personne concernée parce que l'exactitude des données est contestée, il convient de réaliser trois copies «instantanées» des données (par impression, sauvegarde ou gravure sur CD-ROM): une pour la personne concernée, une autre pour le responsable du traitement et la troisième à mettre à disposition du délégué à la protection des données (ou coordinateur de la protection des données) de l'institution concernée. Enfin, il convient d'indiquer clairement dans le système qu'une procédure visant à verrouiller des données a été lancée.

Le CEPD ne peut accepter cette solution que lorsque les données doivent être conservées à titre probatoire (article 15, paragraphe 1, point b) et article 15, paragraphe 1, point c), du règlement) et dans la mesure où il est impossible de procéder dans l'immédiat aux modifications informatiques nécessaires en vue d'une modification du système de gestion existant afin qu'il opère un verrouillage sélectif. Le verrouillage aurait effectivement dans ce cas la conséquence d'affecter plus encore la personne concernée. Par ailleurs, la possibilité de rectifier l'exactitude des données est applicable de façon rétroactive ainsi que les droits y afférents.

## 9. INFORMATIONS AUX PERSONNES CONCERNÉES

Les articles 11 et 12 du règlement énumèrent des informations devant être fournies aux personnes concernées. Ces articles énumèrent une série d'éléments obligatoires et un autre ensemble d'informations. En ce qui concerne les congés, ces deux articles s'appliquent parce que les personnes concernées fournissent elles-mêmes les données, mais des données sont aussi récupérées dans une base de données interne (systèmes des ressources humaines).

Lorsqu'une nouvelle procédure est en cours de mise en œuvre dans une institution/organe, le CEPD propose que chaque membre du personnel concerné reçoive des informations sur ses droits en tant que personne concernée et sur les procédures à suivre afin d'exercer ces droits sur une base individuelle (sous la forme d'un courriel, par exemple) et que les instruments soient accessibles de manière permanente en ligne (via l'intranet) afin de rendre ces informations accessibles à tout moment aux membres du personnel concernés. En ce qui concerne les procédures existantes, les informations ont normalement déjà été fournies aux personnes concernées, mais elles doivent aussi être disponibles sur l'intranet (s'il existe) ou doivent être d'un accès facile pour les personnes concernées.

Les informations à fournir à la personne concernée doivent, au minimum, contenir:

a) l'identité du responsable du traitement;
b) les finalités du traitement auquel les données sont destinées;
c) les destinataires ou les catégories de destinataires des données;
d) le caractère obligatoire ou facultatif de la réponse aux questions ainsi que les conséquences éventuelles d'un défaut de réponse (par exemple, dans le cas de Flexitime, les conséquences d'un défaut de pointage à l'entrée et/ou à la sortie);
e) l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
f) toute information supplémentaire telle que:
    i) la base juridique du traitement auquel les données sont destinées;
    ii) les délais de conservation des données;
    iii) le droit de saisir à tout moment le contrôleur européen de la protection des données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

## 10. MESURES DE SÉCURITÉ

En vertu de l'article 22 du règlement, «*le responsable du traitement met 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 doivent «*notamment […] empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite*».

Cela inclut, entre autres, le fait que les institutions/organes doivent garantir que les données ne sont pas accessibles par d'autres personnes que celles mentionnées comme destinataires, conformément au principe du besoin d'en connaître, ni communiquées à ces personnes.

En outre, eu égard au caractère particulièrement sensible du traitement des données relatives à la santé et compte tenu du fait que les données indiquant l'état de santé d'une personne sont traitées par les services des ressources humaines dans le cadre des procédures de demandes de congés (par exemple, raison de l'absence, formulaires concernant le congé maladie, certificats médicaux, etc.), le CEPD recommande de rappeler à toutes les personnes travaillant au sein des services des ressources humaines et en charge du traitement d'informations relatives à l'état de santé des membres du personnel de traiter ces informations conformément aux principes du secret médical.

Bien que les membres du personnel soient soumis à une obligation de confidentialité générale en vertu de l'article 17 du statut des fonctionnaires (ou du règlement financier d'une agence), le CEPD considère que cette obligation de confidentialité n'est pas suffisamment spécifique pour couvrir le traitement de données relatives à la santé. Le CEPD recommande dès lors que les institutions et les organes préparent des déclarations spécifiques de confidentialité devant être signées par les membres du personnel des ressources humaines, en vertu desquelles ces derniers sont soumis à une obligation de secret professionnel équivalente à celle d'un praticien de la santé, conformément à l'article 10, paragraphe 3, du règlement.

En ce qui concerne le développement de **systèmes Flexitime utilisant la technologie RFID**, le CEPD considère qu'afin d'assurer un niveau élevé de sécurité technologique et organisationnelle d'un système Flexitime, il convient de tenir compte de différents risques potentiels, comme le piratage d'un logiciel ou les dommages physiques causés au matériel informatique et au système. Une telle analyse des risques doit toujours faire partie de la première évaluation afin de proposer des solutions telles que l'application de mesures techniques de sécurité spécifiques ou afin de sécuriser les lieux et restreindre l'accès avant de mettre en œuvre un système RFID.

_____