COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, le 30 octobre 2012 T-PD(2012)12_fr

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL [STE n°108]

(T-PD)

Projet de recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi

INDEX

PROJET DE RECOMMENDATION CM/REC(2011)… DU COMITE DES MINISTRES AUX ETATS MEMBRES SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL UTILISEES A DES FINS D'EMPLOI.

(Adoptée le … 2011 par le Comité des Ministres
lors de la … réunion des Ministres délégués)

Le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Conscient de l'utilisation croissante des nouvelles technologies et des instruments de communication électronique dans les relations entre employeurs et employés et des avantages qui en découlent ;

Estimant, toutefois, que l'utilisation de méthodes de traitement des données, , par les employeurs devrait être gouvernée par des principes destinés à réduire au minimum les risques que de telles méthodes pourraient éventuellement présenter pour les droits et les libertés fondamentales des employés, notamment leur droit à la vie privée , à l'égard du traitement de ses données à caractère personnel ;

Ayant à l'esprit les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (ci-après la Convention 108), ainsi que celles de son Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001, et compte tenu de l'intérêt de convertir ces principes eu égard aux exigences propres au secteur de l'emploi ;

Reconnaissant également que, lors de l'élaboration de principes dans le secteur de l'emploi, il doit être tenu compte aussi bien des intérêts individuels que des intérêts collectifs;

Conscient des traditions différentes existant dans les Etats membres en ce qui concerne la réglementation des divers aspects des relations employeur-employé, la réglementation par voie législative ne constituant qu'une des méthodes utilisées ;

Conscient des changements intervenus à l'échelle internationale dans le monde du travail et des processus de production qui sont liés, du fait notamment du recours aux technologies de l'information et de la communication et de la globalisation des activités et des services ;

Considérant que ces changements appellent à une révision de la Recommandation N° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi en vue de continuer à procurer une protection adéquate des personnes ;

Rappelant les «Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance » adoptés en mai 2003 par le Comité Européen de Coopération juridique (CDCJ) du Conseil de l'Europe et rappelés dans la Résolution 1604 (2008) de l'Assemblée parlementaire du Conseil de l'Europe demeurent pleinement valides et pertinents, et considérant en conséquence qu'il n'est pas nécessaire d'introduire dans une nouvelle Recommandation d'autres principes spécifiques concernant l'utilisation d'instruments de vidéosurveillance ;

Rappelant la Charte sociale européenne (STCE n° 163), dans sa version révisée du 3 mai 1996, ainsi que le Code de conduite du Bureau international du travail de 1997 sur la protection des données personnelles des travailleurs ;

Rappelant la Convention européenne des droits de l'Homme, qui protège en son Article 8 le droit à la vie privée, qui comprend, tel qu'interprété par la jurisprudence pertinente de la Cour européenne des droits de l'homme, les activités de nature professionnelle ;

Recommande aux gouvernements des Etats membres :

- d'assurer que les principes contenus dans la présente recommandation et son annexe, qui remplace la Recommandation R N° (89)2 susmentionnée, soient reflétés dans la mise en œuvre des législations nationales relatives à la protection des données dans le secteur de l'emploi;

- d'assurer, à cette fin, que la présente recommandation soit portée à l'attention des autorités établies conformément à la législation nationale en matière de protection des données et chargées de contrôler l'application de cette législation ;

- de promouvoir l'acceptation et l'application des principes contenus dans l'annexe à la présente Recommandation, également au moyen d'instruments complémentaires tels que des codes de conduite, en assurant une large diffusion de celle-ci auprès des organes représentatifs des employeurs et des employés et en impliquant les concepteurs et fournisseurs de technologies dans les procédés de mise en œuvre de certains principes.

Annexe à la Recommandation

[Partie I – Principes généraux]

1. *Champ d'application et définitions*

1.1. Les principes de la présente recommandation s'appliquent à la collecte et au traitement de données à caractère personnel à des fins d'emploi dans les secteurs public et privé.

Un traitement de données à caractère personnel non-automatisé ne devrait pas être effectué par un employeur dans le but de se soustraire aux dispositions de la présente recommandation.

1.2. Sauf législations nationales contraires, les principes de la présente recommandation s'appliquent, le cas échéant, aux activités des agences pour l'emploi, dans les secteurs public et privé, qui collectent et traitent, également par l'intermédiaire de systèmes d'information en ligne, des données à caractère personnel afin de permettre l'établissement d'un ou de plusieurs contrats de travail simultanés ou à temps partiel entre les personnes qui figurent sur leurs listes et d'éventuels employeurs, ou afin de faciliter les démarches dérivant desdits contrats.

1.3. Aux fins de la présente recommandation :

- «données à caractère personnel» signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée »).

- « traitement automatisé » s'entend de toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, et notamment la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement, la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques aux données ;

- « responsable du traitement » signifie la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données ;

- « destinataire » signifie la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles, y compris lorsque le transfert de données vers l'étranger est effectué par l'intermédiaire de sociétés prestataires;

- « données sensibles » signifie les données à caractère personnel révélant l'origine raciale, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, l'information biométrique, ainsi que les données génétiques, les données liées à la santé ou à la vie sexuelle, les données liées aux condamnations pénales ou incriminations, ou encore les mesures de sécurité [et autres données définies comme sensibles par le droit national], dont le traitement présente un risque grave pour les intérêts, les droits et les libertés fondamentales de la personne concernée.

- « systèmes d'information » signifie tout dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assure(nt), conformément à un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance ;

– « à des fins d'emploi» concerne les rapports entre employés et employeurs relatifs au recrutement des employés, à l'exécution du contrat de travail, à la gestion, y compris les obligations découlant de la loi ou de conventions collectives, ainsi que la planification et l'organisation du travail.

- « employeur » signifie toute personne physique ou morale qui entretient un lien de hiérarchie avec le ou les employés et qui a la responsabilité de l'entreprise ou de l'établissement ;

- « employé » signifie toute personne employée par l'employeur au terme d'un lien de subordination ;

2. *Respect des droits de l'homme, de la dignité humaine et des libertés fondamentales*

Le respect de la protection des données à caractère personnel, contribuant au respect de la dignité humaine, ainsi que des droits et des libertés fondamentales et notamment du droit à la vie privée, devrait être garanti lors du traitement de données à caractère personnel à des fins d'emploi, notamment pour permettre aux employés le développement libre de leur personnalité et afin de préserver la possibilité de relations sociales et individuelles sur leur lieu de travail.

3. *Nécessité, développement de certains principes et simplifications*

3.1. A travers l'utilisation des systèmes et technologies d'information pour la collecte et le traitement de données à caractère personnel à des fins d'emploi l'employeur doit être encouragé à veiller à l'application des principes de sécurité en vue de prévenir ou au moins de réduire le risque d'atteinte aux droits et libertés fondamentales des personnes concernés. Les principes fondamentaux de la Convention 108 sont pleinement applicables aux traitements de données personnelles réalisés au moyen de systèmes d'information et de technologies. Ces principes de base comprennent notamment la qualité des données (article 5), l'interdiction du traitement des données sensibles (article 6), la sécurité des données (article 7) et les garanties dont peuvent bénéficier les personnes concernées (article 8). Il en est de même lorsque ces systèmes et technologies d'information sont appliqués dans le cadre d'un environnement de travail.

3.2. L'employeur devrait être invité à développer des mesures appropriées, y compris organisationnelles, visant à respecter en pratique les principes en matière de traitement des données aux fins d'emploi, et pouvoir le prouver de manière adéquate sur demande des autorités de contrôle.

3.3. Des mesures devraient être adoptées en fonction de la taille de l'entité concernée et de la nature des activités entreprises et tenant également compte des implications possibles pour les personnes concernées.

4. *Collecte des données*

4.1. Les employeurs devraient être encouragés en principe à collecter les données à caractère personnel auprès de la personne concernée. Lorsqu'il convient de traiter des données externes à la relation d'emploi ou de consulter des tiers, notamment s'agissant de références professionnelles, la personne concernée devrait en être informée.

4.2. Les données à caractère personnel collectées par les employeurs à des fins d'emploi devraient être pertinentes et non excessives, compte tenu du type d'emploi ainsi que des besoins évolutifs d'information de l'employeur.

4.3. Au cours d'une procédure de recrutement ou d'avancement des employés les données collectées auprès des candidats devraient se limiter à celles qui sont nécessaires pour évaluer l'aptitude des intéressés et leurs perspectives de carrière.

[Au cours d'une procédure de recrutement, les données personnelles doivent être obtenues uniquement auprès de la personne concernée. Un employeur ne doit pas convaincre la personne concernée de lui accorder l'accès à des informations privées, ou permettre l'accès à toute information médicale par des tiers.]

En tout état de cause, l'employeur est invité à prendre des mesures appropriées afin que, parmi les données facilement accessibles sur des réseaux de communication électronique à disposition du public, seules les données pertinentes, exactes et mises à jour soient utilisées, ce qui éviterait que ces données soient mal interprétées ou traitées de façon déloyale au regard de leur origine. Par ailleurs, la personne concernée devrait être informée et, le cas échéant, son consentement peut être requis.

5. *Enregistrement des données*

5.1. L'enregistrement de données à caractère personnel n'est possible que si les données ont été collectées conformément aux règles définies aux principes 4 et aux principes 14 à 20

et si l'enregistrement est réalisé à des fins d'emploi. Dans le cas contraire, l'employeur devrait s'abstenir d'utiliser les données enregistrées ou de collecter et/ou d'utiliser de telles données.

5.2. Il en est de même en ce qui concerne les données sociales, qui doivent seulement être collectées à des finalités déterminées et accessibles à certaines personnes uniquement.

5.3 Selon la Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage adoptée le 23 novembre 2010, dont les principes sont pleinement applicables ici, les données à caractère personnel utilisées dans le cadre du profilage ne devraient être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. La collecte et le traitement, dans le cadre du profilage, des données à caractère personnel des personnes qui ne peuvent exprimer seules leur consentement libre, spécifique et éclairé devraient être interdits à moins que cela soit dans l'intérêt légitime de la personne concernée ou pour un intérêt public prépondérant, et à condition que des garanties appropriées soient prévues par une loi.

5.4. Lorsque des données appréciatives relatives à la productivité ou à la potentialité des employés sont enregistrées, de telles données ne devraient servir qu'à évaluer les compétences professionnelles. Ces données devraient être fondées sur des évaluations équitables et loyales et devraient être pertinentes, adéquates et non-excessives. La collecte de données et d'informations relative à la vie privée des employés devrait par conséquent être interdite.

6. *Utilisation interne des données*

6.1. Les données à caractère personnel collectées à des fins d'emploi ne devraient être traitées par l'employeur qu'à de telles fins.

6.2. Lorsque des données doivent être traitées ou interconnectés à des fins d'emploi autres que celles pour lesquelles elles ont été initialement collectées, l'employeur devrait être encouragé à prendre des mesures appropriées pour éviter que ces données ne soient mal interprétées dans un contexte différent et pour assurer qu'elles ne soient pas utilisées de manière incompatible avec le but initial. En cas de décision importante concernant l'employé, fondée sur des données ainsi traitées, celui-ci devrait en être avisé.

6.3. Sans préjudice des dispositions du principe 8, lors de changements au sein l'entreprise, de fusions et d'acquisitions, il convient de veiller au respect du principe de spécification de la finalité dans l'utilisation ultérieure des données. Lorsque des modifications substantielles du traitement interviennent, la personne concernée doit en être informée.

7. *Communication de données et utilisation de systèmes d'information aux fins de représentation des employés*

7.1. Conformément aux législations et pratiques nationales et aux conventions collectives, des données à caractère personnel peuvent être communiquées aux représentants des employés, dans la mesure où de telles données sont nécessaires pour permettre à ces derniers de représenter les intérêts des employés.

7.2. Les employeurs devraient être invités à envisager l'utilisation de systèmes et technologies d'information pour des communications à caractère syndical dans le cadre

d’accords spécifiques avec l’employeur, visant à définir au préalable des règles transparentes permettant une utilisation appropriée, ainsi qu’à identifier des garanties à titre de protection d’éventuelles communications confidentielles.

8. *Communication externe et transmission des données*

8.1. Les données à caractère personnel collectées à des fins d'emploi ne devraient être communiquées à des organismes publics pour l’accomplissement de leur mission que dans les limites des obligations légales de l'employeur ou conformément à d'autres dispositions du droit interne.

8.2. La communication de données personnelles à des organismes publics à des fins autres que l'exercice de leurs fonctions officielles ou à des parties autres que des organismes publics, y compris les entreprises du même groupe, ne devrait s'effectuer que :

a. lorsque la communication est nécessaire à des fins d'emploi qui ne seraient pas incompatibles avec les finalités pour lesquelles les données ont été collectées à l'origine et si les employés ou leurs représentants en sont informés ; ou

b. avec le consentement exprès de l'employé ; ou

c. si la communication est autorisée par le droit interne, notamment si cela s’avère nécessaire en cas d’action en justice ou en vue de l’exercice d’un droit devant une instance judiciaire.

8.3. Selon les garanties appropriées prévues par le droit interne, des données à caractère personnel peuvent être communiquées au sein d’un groupe de sociétés afin d’exécuter les obligations prévues par la loi ou par convention collective. Le consentement de l’employé peut aussi être requis.

8.4 Dans le secteur public, la législation nationale prévoyant des dispositions sur la divulgation de données à caractère personnel afin de garantir la transparence ou le contrôle de l’utilisation des ressources et de fonds publics devrait également prévoir des garanties appropriées eu égard au droit au respect de la vie privée et à la protection des données à caractère personnel des personnes, notamment en garantissant le plein respect du principe de finalité et en évitant la divulgation de données à caractère personnel qui ne sont pas pertinentes. La loi devrait également permettre de réconcilier le droit au respect de la vie privée et à la protection des données à caractère personnel avec les exigences de sécurité nationale, de lutte contre le crime, en l’occurrence la corruption et d’autres intérêts protégés par la loi.

9. Données sensibles

9.1. Les données à caractère personnel visées à l'article 6 de la Convention 108, dont le traitement doit en principe être interdit, peuvent néanmoins être traitées, dans des cas particuliers, lorsque cela est indispensable au recrutement ou à l’exécution d’obligations légales dérivant du contrat de travail, à condition que la loi applicable prévoit des garanties appropriées additionnelles.

9.2. Un employé ou un candidat à un emploi ne peut être interrogé sur son état de santé et faire l'objet d'un examen médical qu'aux fins suivantes :

a. déterminer son aptitude à un emploi actuel ou futur ;

b. couvrir les besoins de la médecine préventive ;

c. octroyer des prestations sociales ; ou

d. répondre à une procédure judiciaire.

En principe, le traitement de données génétiques, en particulier pour déterminer l'aptitude professionnelle des employés ou des candidats lors de l'instauration d'un contrat de travail, même avec le consentement de l'intéressé, est interdit. Des dérogations exceptionnelles pourraient être seulement prévues lorsque la loi applicable prévoit des garanties appropriées additionnelles, qui devraient également prévoir une implication préalable des autorités de contrôle, dans le seul but d'adopter, à la demande de l'employé, les mesures nécessaires à son état de santé, à l'état de santé de tiers et aux conditions de sécurité ou de travail.

9.3. Les données de santé et - lorsque leur traitement est licite - les données génétiques ne peuvent être collectées auprès d'autres sources que l'employé lui-même sans le consentement exprès de ce dernier ou conformément aux dispositions du droit interne.

9.4. Les données de santé couvertes par le secret médical et - lorsque leur traitement est licite - les données génétiques, ne peuvent être traitées que par le personnel soumis lié par le secret médical.

Ces informations ne devraient être communiquées à des membres du service du personnel que si cela est indispensable à la prise de décisions par ce service et conformément au droit interne.

9.5. Les données de santé couvertes par le secret médical et - lorsque leur traitement est licite - les données génétiques devraient être enregistrées séparément des autres catégories de données détenues par l'employeur. Des mesures de sécurité devraient être prises pour éviter que des personnes étrangères au service médical n'aient accès à ces données.

9.6. Le droit d'accès de la personne concernée à ses données médicales ne devrait pas faire l'objet de restrictions, à moins que l'accès à de telles données ne puisse porter une grave atteinte à la personne concernée ; dans ce cas, ces données pourraient lui être communiquées par l'intermédiaire du médecin de son choix.

9.7. L'employeur devrait traiter les éventuelles données sur la santé relatives à des tiers si cela est indispensable à l'exécution des obligations prévues par la loi ou par la convention collective, dans le respect des garanties prévues pour les données sur la santé des employés.

10. *Transparence du traitement*

10.1. Les employés devraient pouvoir recevoir des informations concernant les données à caractère personnel détenues par l'employeur, soit directement, soit par l'intermédiaire de ses représentants.

Outre les informations concernant l'identité et la résidence habituelle ou lieu d'établissement, ces informations devraient spécifier les finalités du traitement des données mis en œuvre par le responsable de traitement, c'est-à-dire l'employeur, les données traitées, les destinataires ou catégories de destinataires de ces données à caractère personnel et les moyens d'exercer les droits énoncés à l'article 8 de la Convention 108, ainsi que toute autre information nécessaire pour garantir un traitement loyal et licite des données.

Dans ce contexte, une description particulièrement claire et complète devrait être fournie concernant la typologie et l'utilisation potentielle des données à caractère personnel qui peuvent être collectées au moyen de systèmes et technologies d'information et qui permettent à l'employeur de contrôler indirectement les employés. Des informations claires et précises devraient être fournies au regard des formes particulières de traitement des données à caractère personnel des employés prévues dans la partie II de cette Annexe.

10.2. Ces informations devraient également faire mention des droits de l'employé au regard de ses données, tels qu'ils sont prévus au principe 11 de la présente recommandation, ainsi que des modalités d'exercice des droits.

10.3. Les informations devraient être fournies et mises à jour en temps utile et, en tout état de cause, avant que l'employé ne réalise l'activité ou le comportement qui est visé, puis mises à disposition au moyen de systèmes d'information habituellement utilisés par l'employé.

11. *Droit d'accès et de rectification*

11.1. Tout employé ne doit pas être soumis à une décision l'affectant de manière significative, qui serait uniquement basée sur un traitement automatisé de données, sans que son point de vue soit pris en compte.

11.2 En outre, il ou elle doit pouvoir obtenir, à sa demande, à intervalle raisonnable et sans délai ou frais excessifs, la confirmation d'un traitement de données le ou la concernant, la communication sous une forme intelligible des données traitées, toutes informations disponibles sur leur origine, ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements. Tout employé doit également obtenir, à sa demande, connaissance du traitement qui sous-tend le traitement de données dont les résultats lui sont appliqués et obtenir, le cas échéant, la rectification ou l'effacement de telles données lorsqu'elles sont traitées en violation du droit interne ou des principes énoncés dans cette Convention, notamment en cas d'inexactitude.

A cette fin, particulièrement pour les entités de grande dimension ou dispersées sur le territoire, l'employeur devrait prévoir des procédures préventives d'ordre général afin de garantir que le contrôle soit adéquat et rapide en cas d'exercice de ces droits.

11.3. Le droit d'accès devrait également être garanti s'agissant des données d'évaluation, y compris celles relatives aux appréciations de la productivité ou du potentiel de l'employé, prévues au principe. 5.4, au moins lorsque le processus d'appréciation est terminé, sans préjudice du droit de l'employeur ou de tiers de se défendre ; même si l'employé ne peut les rectifier directement, les appréciations purement subjectives devraient pouvoir être contestées selon les modalités prévues par le droit interne.

11.4 Des dérogations aux droits auxquels il est fait référence aux paragraphes 11.1 et 11.2 peuvent intervenir lorsqu'elles sont prévues par une loi accessible et prévisible et constituent une mesure nécessaire dans une société démocratique, tel que le prévoit l'article 9 de la Convention 108, à la protection de la sûreté de l'Etat, à la sécurité publique, à des intérêts économiques et financiers importants de l'Etat ou à la prévention et à la répression des infractions pénales, ainsi qu'à la protection de la personne concernée et des droits et libertés d'autrui, notamment la liberté d'expression. A cet égard, d'après la Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage adoptée le 23 novembre 2010, « lorsque cela est nécessaire dans une société démocratique pour des raisons de sécurité nationale, de sûreté publique, de défense des intérêts monétaires du pays, de prévention ou de répression des infractions pénales, ou

à la protection des personnes concernées ou des droits et libertés d'autrui, les Etats membres n'appliquent pas les dispositions des chapitres 3, 4 et 5 (conditions régissant la collecte et le traitement de données personnelles dans le cadre du profilage, information et droits de la personne concernée) de la présente recommandation, pour autant que cela soit prévu par la loi ».

11.5. Par ailleurs, dans le cas d'une enquête interne effectuée par l'employeur, l'exercice de ces droits peut être différé jusqu'à la conclusion de cette enquête, si cet exercice risque de nuire au résultat de l'enquête. Cependant, un signalement anonyme ne saurait être à l'origine d'enquêtes internes, sauf si ce signalement est circonstancié et concerne de graves violations identifiées par le droit national ou par une décision de l'autorité de contrôle.

11.6. Sauf dispositions nationales contraires, l'employé devrait pouvoir désigner une personne de son choix pour l'assister lors de l'exercice de son droit d'accès ou pour exercer ce droit en son nom.

11.7. Si un employé se voit refuser l'accès aux données le concernant ou la possibilité de rectifier ou d'effacer certaines de ces données, une voie de recours devrait être prévue par le droit interne.

12. Sécurité des données

12.1. Les employeurs ou les entreprises auprès desquelles les données peuvent être sous-traitées devraient être invités à mettre en oeuvre des mesures techniques et organisationnelles appropriées et mises à jour lors du développement de nouvelles technologies pour garantir la sécurité et la confidentialité des données à caractère personnel enregistrées à des fins d'emploi, contre la modification, la perte ou la destruction accidentelles ou non autorisées de données à caractère personnel, ainsi que contre l'accès à ces données, leur diffusion ou leur divulgation non autorisés.

12.2. Le service du personnel ainsi que toute autre personne intervenant dans le traitement des données devraient être tenus informés de ces mesures et de la nécessité de les respecter.

13. Conservation des données

13.1. Un employeur ne devrait pas conserver des données à caractère personnel pendant une période plus longue que ne le justifient les finalités définies au paragraphe 1.3 ou que ne le nécessite l'intérêt d'un employé actuel ou d'un ancien employé.

13.2. Les données à caractère personnel fournies à la suite d'un acte de candidature devraient en principe être effacées dès qu'il devient clair qu'une offre d'emploi n'interviendra pas.

13.3. Lorsque de telles données sont conservées en vue d'une demande d'emploi ultérieure, l'intéressé devrait en être informé en temps utile et les données devraient être effacées à sa demande.

Lorsque, pour soutenir d'éventuelles actions en justice, il est nécessaire de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que pendant la période la plus courte possible.

13.4. Les données à caractère personnel traitées aux fins d'une enquête interne réalisée par l'employeur et qui n'a entraîné l'adoption d'aucune mesure négative à l'égard des

employés doivent, en principe, être effacées dans les meilleurs délais, sans préjudice de l'exercice du droit d'accès jusqu'à ce qu'elles soient effacées.

[Part II – Formes particulières de traitement]

14. *Systèmes et technologies d'information pour le traitement de données à caractère personnel et le contrôle du travail des employés, incluant la vidéosurveillance*

14.1 L'introduction et l'utilisation de systèmes et technologies d'information utilisés directement et essentiellement afin de contrôler à distance le travail, le comportement ou la [localisation] des employés aux fins de la production, de la sécurité ou de l'organisation du travail de l'établissement, ne devraient en principe pas être autorisées lorsqu'elles conduisent à une surveillance délibérée et systématique d'un employé en particulier, ou d'un groupe d'employés spécifiques, à l'exception de l'indisponibilité de mesures alternatives qui soient moins intrusives, [et pour autant qu'une autorisation préalable a été délivrée par une autorité nationale de contrôle]. Les employés ou leurs représentants, conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives pertinentes, devraient être préalablement informés ou consultés à l'introduction ou à la modification d'un système de vidéosurveillance. Lorsque la procédure de consultation révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine des employés, leur accord doit être recherché. En cas de litige ou de revendication, les employés devraient pouvoir se servir des enregistrements réalisés.

14.2 Lors de l'introduction, de la modification et du fonctionnement de systèmes et technologies d'information utilisés pour la collecte et le traitement de données à caractère personnel nécessaires aux fins de la production, de la sécurité ou de l'organisation du travail, les employés ou leurs représentants, conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives pertinentes, devraient être préalablement informés ou consultés.

15. Dispositifs d'alerte professionnelle

Les dispositifs d'alerte professionnelle peuvent également avoir un impact sur les droits et les libertés fondamentales des personnes concernées. Ces dispositifs, qui peuvent permettre aux salariés d'une entreprise de signaler des activités illégales, des problèmes d'ordre financier, de corruption ou de concurrence, s'inscrivent dans un cadre précis. Le champ d'application de ces dispositifs doit être restreint et ne doit pas avoir une portée générale et ne doit pas viser le respect de l'ensemble des dispositions législatives ou réglementaires ou des règles internes établies par l'organisme. Si des faits graves, hors du champ sont signalés, notamment liés à l'intégrité morale ou physique des salariés, l'alerte doit être immédiatement réorientée vers le responsable compétent (directeur financier, directeur des ressources humaines).

16. Utilisation de l'Internet et des messages électroniques sur le lieu de travail

16.1 Eu égard à l'éventuel traitement de données à caractère personnel figurant sur des pages du réseau Internet ou Intranet, les employeurs devraient être encouragés à prévenir des atteintes injustifiées au droit au respect de la vie privée et à la protection des données à caractère personnel des individus.

Les personnes concernées devraient être convenablement et périodiquement informées, conformément aux principes 4 et 10 de la Recommandation, notamment lorsque des

mesures disciplinaires sont envisagées sur la base des fichiers de contrôle constitués. Les informations doivent porter sur la finalité du dispositif et la durée de conservation ou de sauvegarde des données de connexion. Ces informations doivent également concerner l'archivage des messages électroniques.

16.2 En ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel figurant sur des pages du réseau Internet ou Intranet consultées par l'employé, il conviendrait d'adopter les mesures préventives, telles que la configuration de systèmes ou l'utilisation de filtres qui peuvent empêcher certaines opérations, le cas échéant, et la graduation des éventuels contrôles relatifs aux données à caractère personnel, moyennant dans un premier temps des contrôles par sondages non individuels sur des données anonymes ou groupées. Les personnes concernées devraient être régulièrement informées, conformément au principe 10 de la Recommandation et plus généralement, les employés devraient avoir été préalablement informés de la politique suivie par l'entreprise ou l'institution visant à mener de telles activités de contrôle.

16.3 L'accès aux messages électroniques professionnels des employés qui ont été préalablement informés de l'existence de cette éventualité, ne peut survenir qu'en conformité avec la législation et si cela est strictement nécessaire pour des raisons de sécurité et de fonctionnement. L'employeur devrait être invité à éviter toute sorte d'accès injustifié aux messages envoyés et reçus par l'employé. Il devrait être encouragé à prendre les mesures nécessaires et à prévoir les procédures appropriées visant à permettre, en cas d'absence de l'employé, l'accès aux messages électroniques professionnels lorsqu'un tel accès est absolument nécessaire d'un point de vue professionnel, de la façon la moins intrusive possible et après avoir informé l'employé.

17. Appareils permettant de géolocaliser les employés

Tandis que les appareils permettant de localiser les employés peuvent être utilisés dans l'intérêt des employés (par exemple pour déterminer un accident du travail) leur utilisation ne doit pas conduire à un contrôle permanent des employés. Considérant les risques d'atteinte aux droits et aux libertés des personnes que présente l'utilisation de ces appareils, l'employeur devrait être invité à prendre toutes les garanties nécessaires. Il doit notamment accorder une attention particulière aux finalités pour lesquelles de tels appareils sont utilisés.

Si, en vertu des spécificités dues à l'activité professionnelle, conformément aux instructions ou après s'être assuré que l'employeur en connaisse au préalable les modalités et en accord avec ce dernier, l'employé est amené à utiliser des appareils professionnels en dehors de l'entreprise ou de l'institution, et qu'en vertu de cette utilisation, l'employeur peut localiser l'employé, la collecte et d'autres traitements de données à caractère personnel résultant de cette possibilité doivent être exclusivement limités à la stricte vérification de l'exécution des tâches professionnelles ou d'autres aspects en termes d'organisation.

L'employeur doit prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux personnes concernées. La consultation préalable des organes représentatifs devrait être assurée.

18. Données biométriques

L'accès à de telles données doit être soumis à des exigences de sécurité et de proportionnalité. A cet égard, une attention particulière devrait être accordée aux implications d'un enregistrement effectué dans une base de données centralisée ou à des systèmes alternatifs basés sur des supports mis à la disposition exclusive de l'intéressé.

La collecte puis le traitement de données biométriques ne devraient être réalisés que lorsque nécessaire à la protection des intérêts légitimes de l'employeur, des employés ou des tiers, devraient s'accompagner de garanties appropriées, en particulier en ce qui concerne la sécurité et être conformes aux règles de santé et d'hygiène. Les employés doivent avoir été préalablement informés de la politique de l'entreprise ou de l'institution concernant la collecte puis le traitement de telles données.

La collecte puis le traitement de données biométriques ne devraient être réalisés qu'après avoir obtenu l'autorisation préalable des autorités nationales de contrôle.

19. Tests psychologiques, analyses et procédures analogues

Le recours à des tests, à des analyses et à des procédures analogues effectués par des professionnels spécialisés et destinés à évaluer le caractère ou la personnalité d'une personne ne devraient se faire qu'en cas de stricte nécessité et ne devraient pas se faire sans son consentement, à moins que d'autres garanties appropriées ne soient prévues par le droit interne. La personne concernée devrait pouvoir, si elle le désire, être informée au préalable des modalités d'utilisation des résultats de ces tests, analyses ou procédures analogues et, par la suite, de leur contenu. Ces procédures peuvent être soumises au contrôle des autorités nationales de contrôle.

20. Autres traitements de nature à présenter des risques spécifiques au regard des droits des employés

L'employeur devrait adopter des mesures appropriées pour évaluer l'impact d'éventuels traitements de données souhaités et qui peuvent présenter des risques d'atteintes spécifiques aux droits et libertés fondamentales des personnes concernées, et en particulier au droit au respect de la vie privée, à la dignité humaine et à la protection des données à caractère personnel, et pour traiter ces données de la façon la moins intrusive possible. L'accord des représentants des employés devrait être recherché préalablement à l'introduction ou à la modification de tels systèmes et technologies d'information lorsque la procédure de consultation mentionnée au principe 14.2 révèle une possibilité d'atteinte, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationales.