Strasbourg, le 15 Avril 2014 T-PD(2013)5rev_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(2013)… DU COMITE DES MINISTRES AUX ETATS MEMBRES SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL UTILISEES A DES FINS D'EMPLOI.

(Adoptée le … 2014 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 employeur et employés et des avantages qui en découlent ;

Estimant, toutefois, que l'utilisation de méthodes de traitement des données, par l' employeur 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 ;

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 l'application de ces principes 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 autres intérêts (individuels, ou collectifs, privés et publiques);

Considérant que les données à caractère personnel dans les documents officiels détenus par une autorité publique ou un organisme public peuvent être divulguées par l'autorité ou l'organisme conformément à la législation nationale à laquelle l'autorité ou organisme public est soumis, afin de concilier le droit d'accès à ces documents officiels avec le droit à la protection des données à caractère personnel conformément à la présente Recommandation;

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

Conscient des changements intervenus à l'échelle internationale dans le monde du travail et activités qui y sont liés, du fait notamment du recours accru aux technologies de l'information et de la communication (TICs) et de la mondialisation de l'emploi 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 assurer un niveau de protection adéquat des personnes dans le secteur de l'emploi ;

Rappelant l'article 8 de la Convention européenne des droits de l'Homme, qui protège le droit à la vie privée, comprenant, tel qu'interprété par la Cour européenne des droits de l'homme, les activités de nature professionnelle et/ou commerciale;

Rappelant l'application des principes établis par d'autres recommandations pertinentes du Conseil de l'Europe, en particulier la Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, la Recommandation R(97)5 relative à la protection des données médicales et la Recommandation R(92)3 sur les tests et le dépistage génétiques à des fins médicales ;

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 par le Comité Européen de Coopération juridique (CDCJ) du Conseil de l'Europe en mai 2003 et mentionnés dans la Résolution 1604 (2008) de l'Assemblée parlementaire du Conseil de l'Europe qui sont particulièrement pertinents ;

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 à caractère personnel des travailleurs ;

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, ainsi que dans d'autres branches de toute loi portant sur l'utilisation des données à caractère personnel à des fins d'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 ;

- et de promouvoir par ailleurs l'acceptation et l'application des principes contenus dans l'annexe de la présente Recommandation, au moyen d'instruments complémentaires tels que des codes de conduite, en s'assurant que ces principes soient bien assimilés/ admis et mis en application par tous les intervenants du secteur de l'emploi, incluant les organes représentatifs de l'employeur et des employés et pris en compte dans la conception, le déploiement et l'utilisation des TICs dans ce secteur.

Annexe à la Recommandation

Partie I – Principes généraux

1. Champ d'application

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

1.2. Sauf législations nationales contraires, les principes de la présente recommandation s'appliquent aussi aux activités des agences pour l'emploi, dans les secteurs public et privé, qui traitent des données à caractère personnel afin de permettre l'établissement d'un ou de plusieurs contrats de travail simultanés, y compris de contrats à temps partiel, entre les personnes concernées qui figurent sur leurs listes et d'éventuels employeurs, ou afin de faciliter les démarches pour les employeurs dérivant desdits contrats.

1bis. Définitions

Aux fins de la présente recommandation :

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

– « traitement» 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, l'interconnexion, la communication, la mise à disposition, l'effacement, la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques aux données ; lorsqu'aucun procédé automatisé n'est utilisé, le traitement de données s'entend des opérations effectuées au sein d'un ensemble structuré établi selon tout critère qui permet de rechercher des données à caractère personnel ;

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

– « sous-traitant » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

– « destinataire » signifie la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles ;

– « les données sensibles » couvrent les données génétiques ou les données concernant des infractions, condamnations pénales et mesures de sûreté connexes, les données biométriques identifiant un individu de façon unique ainsi que les données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle ;

– « systèmes d'information » signifie tout dispositif isolé ou groupe de dispositifs interconnectés ou liés entre eux, qui assurent - 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 et à son encadrement, y compris à l'exécution des obligations découlant de la loi ou de conventions collectives, ainsi qu'à la planification et l'organisation du travail ou la fin des rapports de travail. Les conséquences de la relation contractuelle peuvent s'étendre au-delà du terme du contrat de travail.

– « employeur » signifie toute personne physique ou morale, l'autorité publique ou l'agence engagée dans un lien d'emploi avec l'employé ou un candidat à un emploi et détenant la responsabilité légale de l'entreprise ou de l'établissement ;

– « employé » ou « candidat à l'emploi » signifie toute personne concernée engagée dans une relation de travail avec un employeur ;

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

Le respect de la dignité humaine, de la vie privée et de la protection des données à caractère personnel devrait être garanti lors du traitement des données 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. Application des principes de traitement

[3.1. Les employeurs devraient veiller à ce que le traitement des données à caractère personnel ne porte que sur les données strictement nécessaires pour atteindre l'objectif déterminé dans les cas individuels concernés et le cas échéant procéder à l'anonymisation des données moyennant le respect des conditions et garanties additionnelles prévues par le droit interne ou procéder à la pseudonymisation des données lorsque l'anonymisation n'est pas possible.]

3.2. Les employeurs devraient développer des mesures appropriées, visant à respecter en pratique les principes et obligations en matière de traitement des données aux fins d'emploi. A la demande des autorités de contrôle, l'employeur devrait être en mesure de démontrer qu'il est en conformité avec des tels principes et obligations. Ces mesures devraient être adaptées au volume et à la nature des données traitées et aux activités entreprises ; elles tiendront également compte des conséquences possibles pour les droits et les libertés fondamentales des personnes concernées.

4. Collecte des données

4.1. L'employeur devrait collecter les données à caractère personnel directement auprès de la personne concernée. Lorsqu'il est nécessaire, licite, loyal et approprié de traiter des données collectées auprès des tiers, par exemple pour obtenir des références professionnelles, la personne concernée devrait en être dûment informée.

4.2. Les données à caractère personnel collectées à des fins d'emploi devraient être pertinentes et non excessives, eu égard à la nature de l'emploi ainsi qu'aux besoins légitimes de l'employeur en lien direct avec ses activités et le cas échéant moyennant le respect des conditions et garanties additionnelles prévues par le droit interne.

4.3. L'employeur doit s'abstenir de chercher à accéder à des données à caractère personnel que l'employé partage et qui ne sont pas liées à l'évaluation des capacités du dit employé à remplir ses fonctions.

4.4. L'employeur doit prendre les mesures appropriées pour veiller à ce que les données à caractère personnel mises en ligne (sur le site de l'entreprise par exemple) et accessibles au public, soient pertinentes, exactes et à jour. L'employeur doit veiller à ce que ces données ne soient pas traitées dans un contexte autre que celui dans lequel elles ont été publiées.

4.5. Les données relatives à la santé ne peuvent être collectées qu'aux fins prévues au principe 9.2 de la présente Recommandation.

[5. Enregistrement des données

5.1. L'enregistrement de données à caractère personnel à des fins d'emploi n'est possible que si les données ont été collectées conformément aux règles définies aux principes 4, 9 et 14 à 20 de la présente Recommandation. Ces données devraient être pertinentes, adéquates et non-excessives.

5.2. Lorsque des données d'évaluation relatives à la productivité ou à la capacité des employés sont enregistrées, de telles données ne devraient servir qu'à évaluer les compétences professionnelles.]

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. L'employeur devrait adopter des politiques de protection des données, des règles et/ou d'autres instruments relatifs à l'usage interne des données à caractère personnel.

6.3. Lorsque des données doivent être traitées à des fins d'emploi mais pour des finalités autres que celles pour lesquelles elles ont été initialement collectées, l'employeur devrait prendre des mesures appropriées pour éviter que ces données ne soient mal interprétées dans un contexte différent et en informer l'employé.

6.4. Sans préjudice des dispositions du principe 8, lors de changements au sein de l'entreprise, de fusions et d'acquisitions, il convient de veiller au respect des principes de proportionnalité et de 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 aux représentants des employés, y compris l'utilisation de systèmes et technologies d'information

7.1. Conformément aux législations et pratiques nationales et aux conventions collectives, des données à caractère personnel peuvent être communiquées aux représentants des employés, uniquement si de telles données sont nécessaires pour permettre à ces derniers de représenter de façon appropriée les intérêts des employés concernés ou si elles sont nécessaires afin de garantir l'exécution et la supervision des obligations prévues par les conventions collectives.

7.2. Conformément aux législations et pratiques nationales l'utilisation de systèmes et technologies d'information pour la communication des données aux représentants des employés devrait faire l'objet d'accords spécifiques avec l'employeur, visant à définir au préalable des règles transparentes stipulant leur utilisation et garantissant la protection des communications confidentielles.

8. Communication externe

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

8.2. La communication de données à caractère personnel à des organismes publics à d'autres fins ou à d'autres parties, y compris les entreprises du même groupe, ne devrait s'effectuer que :

> a. moyennant le respect des conditions et garanties additionnelles prévues par le droit interne, 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 concernés ou leurs représentants, selon le cas, en sont informés ; ou

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

c. si la communication est prévue par le droit interne.

8.3. La communication de données à caractère personnel au sein d'un groupe d'entreprises n'est licite que si elle est nécessaire à l'exécution des obligations légales ou des conventions collectives, moyennant le respect des conditions et garanties additionnelles prévues par le droit interne. Le consentement de l'employé peut aussi être requis.

8.4 En ce qui concerne le secteur public, les dispositions relatives à la divulgation de données à caractère personnel afin d'assurer la transparence du gouvernement et de toute autre autorité publique ou organisme et / ou de surveiller l'utilisation correcte des fonds et ressources publiques, devraient 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 employés.

9. Traitement de données sensibles

9.1. Le traitement des données sensibles au sens du principe 1bis de la présente Recommandation, est permis uniquement dans des cas particuliers, lorsque cela est indispensable pour un recrutement spécifique ou à l'exécution d'obligations légales dérivant du contrat de travail. Le traitement est également subordonné à la loi applicable prévoyant des garanties appropriées additionnelles, venant compléter celles de la Convention 108 et de la présente Recommandation. Les garanties appropriées doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales des employés concernés, notamment le risque de discrimination. Le traitement des données biométriques est sujet aux dispositions du principe 18 de cette Recommandation.

9.2. Conformément au droit interne un employé ou un candidat à un emploi peut être interrogé sur son état de santé et/ou faire l'objet d'un examen médical uniquement aux fins de :

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

b. couvrir les besoins de la médecine préventive ;

c. garantir sa réadaptation appropriée au poste de travail ou en tout état de cause afin de s'adapter aux exigences de l'environnement professionnel ;

d. sauvegarder les intérêts vitaux de la personne concernée ou des autres employés ou d'autres personnes ;

e. octroyer des prestations sociales ; ou

f. répondre à une procédure judiciaire.

Le traitement de données génétiques, pour déterminer par exemple l'aptitude professionnelle des employés ou des candidats est interdit, même avec le consentement de l'intéressé.
Le traitement de données génétiques peut exceptionnellement être prévu par le droit interne et moyennant des garanties appropriées, en particulier pour éviter toute atteinte grave à la santé de la personne concernée ou de tiers.

9.3. Les données de santé et - lorsque leur traitement est licite - les données génétiques, ne devraient être collectées qu'auprès de l'employé concerné sauf dispositions contraires prévues par la loi, moyennant des garanties appropriées.

9.4. Les données de santé couvertes par le secret médical ne devraient être accessibles et traitées que par du personnel lié par le secret médical ou par d'autres règles régissant le secret professionnel et les obligations de confidentialité. Ces données devraient :

a. se rapporter directement à l'aptitude de l'employé à exercer ses fonctions, ou

b. être nécessaires pour prendre des mesures en faveur de la santé de l'employé ou

c. être nécessaires pour prévenir un risque pour d'autres personnes.

Lorsque ces données sont communiquées à l'employeur, cette communication devrait être faite aux ayants droit comme l'administration du personnel, de la santé et de la sécurité au travail et l'information ne devrait être communiquée que si elle est indispensable pour la prise de décision par l'administration du personnel, conformément au droit interne.

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

9.6. Le droit d'accès des employés à leurs données de santé ne devrait pas faire l'objet de restrictions, à moins que l'accès à de telles données ne puisse porter une grave atteinte à l'employé. Une telle restriction doit être conforme aux dispositions prévues par le droit interne. Les données pourraient alors être communiquées à l'employé par l'intermédiaire du médecin de son choix.

9.7. En aucun cas les données de santé relatives à des tiers ne feront objet d'un traitement, à moins que la personne concernée n'ait donné au préalable son consentement non-équivoque, et que ce traitement ne soit autorisé par l'autorité de contrôle compétente ou que la collecte des données ne soit indispensable à l'exécution des obligations légales.

10. Transparence du traitement

10.1. L'employé devrait pouvoir être en mesure d'obtenir des informations sur les données à caractère personnel détenues par son employeur. Ces informations pourraient lui être fournies directement ou par l'intermédiaire de ses représentants.

Sauf les informations concernant le nom de l'employé et sa résidence habituelle ou son lieu d'établissement –l'employeur devrait fournir à l'employé les informations suivantes :

- une liste complète des données qui seront traitées et une description des finalités du traitement,
- les destinataires ou catégories de destinataires de ces données,
- les moyens d'exercer les droits énoncés au paragraphe 11 de la présente recommandation, sans pour autant porter préjudice à des moyens plus favorables prévus dans le droit interne ou le système législatif,
- toute autre information nécessaire pour garantir un traitement loyal et licite des données.

Dans ce contexte, devrait être fournie une description particulièrement claire et complète des catégories des données à caractère personnel qui peuvent être collectées au moyen de systèmes et technologies d'information et de communication telle que la vidéosurveillance et de leur utilisation potentielle. Ce principe s'applique pour toutes les formes particulières de

traitement des données à caractère personnel prévues à la partie II de la présente Recommandation.

10.2. Les informations devraient être fournies sous une forme accessible et tenues à jour. En tout état de cause, ces informations devraient être fournies avant que l'employé n'exerce effectivement l'activité ou l'action prévue, et être mises à disposition au moyen des systèmes d'information habituellement utilisés par l'employé.

11. Droit d'accès, de rectification et d'objection

11.1 Les employés devraient pouvoir obtenir, à leur demande, à intervalle raisonnable et sans délai excessif, la confirmation d'un traitement de données les concernant. La communication devrait être faite sous une forme intelligible, inclure toutes informations disponibles sur l'origine des données, ainsi que toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements, en particulier les informations prévues au paragraphe 10.

11.2 Les employés devraient avoir le droit d'obtenir la rectification ou l'effacement de leurs données à caractère personnel en cas d'inexactitude et/ou lorsqu'elles sont traitées en violation du droit interne ou des principes énoncés dans cette Recommandation. Ils devraient également être autorisés à s'opposer à tout moment au traitement des données à caractère personnel les concernant, à moins que ce traitement ne soit nécessaire à des fins d'emploi ou ne soit prévu par la loi.

11.3. Le droit d'accès devrait également être garanti s'agissant des données d'évaluation, y compris celles relatives aux appréciations de la performance, de la productivité ou du potentiel de l'employé, au plus tard lorsque le processus d'appréciation est terminé, sans préjudice du droit de défense de l'employeur ou des tiers impliqués. Bien que ces données ne puissent être directement corrigées par l'employé, les évaluations purement subjectives devraient pouvoir être contestées selon les modalités prévues par le droit interne.

11.4. Les employés ne doivent pas être soumis à une décision les affectant de manière significative, qui serait uniquement basée sur un traitement automatisé de données, sans que leur point de vue ne soit pris en compte.

11.5. Un employé doit également obtenir, à sa demande, des informations concernant les finalités du traitement des données, les résultats de ce traitement et les moyens par lesquels ces résultats l'affectent.

11.6. Des dérogations aux droits auxquels il est fait référence aux paragraphes 11.1, 11.3 et 11.4 peuvent être admises lorsqu'elles sont prévues par une loi et constituent une mesure nécessaire dans une société démocratique, 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.

11.7. 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 l'exercice de ces droits peut nuire/mettre en péril l'enquête.

11.8. 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, de rectification ou d'effacement de ses données ou afin d'exercer ces droits en son nom.

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

12. Sécurité des données

12.1. L'employeur ou les entités, auprès desquelles les données peuvent être sous-traitées, devraient mettre en œuvre des mesures techniques et organisationnelles, qui seront mises à jour si cela s'avère nécessaire, en vue des examens périodiques d'une évaluation des risques et des politiques de sécurité. De telles mesures devraient 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 autorisées.

12.2 L'employeur assure de manière adéquate la sécurité des données lors de l'utilisation des TICs pour le traitement de données à caractère personnel à des fins d'emploi.

12.3. 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 traiter des données à caractère personnel pendant une période plus longue que ne le justifient les finalités définies au principe 1.3. ou que ne le nécessite l'intérêt d'un employé en poste 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 que la candidature ne sera pas retenue.

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 intenter ou soutenir une action en justice ou pour toute autre finalité légitime, il est indispensable de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que pour la période nécessaire à l'action en justice.

13.3. Les données à caractère personnel traitées aux fins d'une enquête interne réalisée par un employeur et qui n'a entraîné l'adoption d'aucune sanction à l'égard des employés devraient être effacées dans un délai raisonnable, sans préjudice de l'exercice du droit d'accès de l'employé jusqu'à ce qu'elles soient effacées.

Partie II – Formes particulières de traitement

14. Systèmes et technologies d'information pour le contrôle des employés, incluant la vidéosurveillance

14.1 L'introduction et l'utilisation des TICs afin de contrôler les employés doivent être faites en respectant les principes de légitimité, de pertinence et de proportionnalité, uniquement lorsqu'il y a impossibilité d'utiliser d'autres méthodes alternatives de traitement qui sont moins intrusives pour la vie privée et lorsqu'ils sont accompagnés de garanties appropriées. Les employeurs devraient établir un juste équilibre entre le droit des employés au respect de la vie privée et l'intérêt de l'employeur de protéger ses droits de propriété.

14.2 L'utilisation des tels systèmes directement et essentiellement afin de contrôler à distance le travail et le comportement des employés, ne doit pas être autorisée lorsqu'elle conduit à une surveillance délibérée et systématique d'un employé en particulier, ou d'un groupe spécifique d'employés. Des exceptions à ce principe pourraient être envisagées, avec des garanties appropriées, lorsque la surveillance n'est pas l'objectif principal poursuivi par l'employeur, mais uniquement une conséquence indirecte d'une surveillance nécessaire aux fins de la production, de la sécurité, de l'organisation du travail de l'établissement ou de la protection de la santé. L'utilisation de tels dispositifs, notamment de vidéosurveillance, dans des endroits qui portent atteinte à la vie intime des employés n'est pas autorisée.

14.3 En cas de litige ou d'action en justice, les employés devraient pouvoir obtenir la copie des enregistrements réalisés.

15. Mécanismes internes de signalement

Lorsque l'employeur est tenu par la loi ou les règles internes de mettre en œuvre des mécanismes internes de signalement, tels que les numéros d'urgence, il doit assurer la protection des données à caractère personnel de toutes les parties concernées. En particulier, l'employeur doit garantir la confidentialité à l'égard de l'employé qui signale les comportements illicites ou contraires à l'éthique (tel qu'un donneur d'alerte). Les données à caractère personnel des parties en cause doivent être utilisées uniquement aux fins des procédures internes appropriées relatives aux dits signalements, à la loi ou à l'ordre judiciaire.

Le cas échéant, l'employeur doit permettre le signalement anonyme. Cependant, un signalement anonyme ne saurait être l'unique origine d'enquêtes internes, sauf si ce signalement est dûment circonstancié et concerne de graves infractions au droit interne.

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

16.1 L'employeur devrait éviter de porter des atteintes injustifiées et déraisonnables au droit au respect de la vie privée de l'employé. Ce principe s'étend à tous les dispositifs techniques et aux TICs utilisés par un employé. Les personnes concernées devraient être convenablement et périodiquement informées à l'aide d'une déclaration claire en matière de respect de la vie privée conformément au principe 10 de la Recommandation. L'information fournie devrait être mise à jour et inclure la finalité du traitement, la durée de conservation des données collectées ainsi qu'à la sauvegarde des données de connexion et à l'archivage des messages électroniques.

16.2 En ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel relatives aux pages Internet ou Intranet consultées par l'employé, il conviendrait d'une part d'adopter des mesures préventives, telles que la configuration de systèmes ou l'utilisation de filtres qui peuvent empêcher certaines opérations, et d'autre part de prévoir éventuellement des contrôles des données à caractère personnel, effectués de manière graduée et utilisant dans un premier temps par sondages non individuels des données anonymes ou agrégées.

16.3 L'accès aux messages électroniques professionnels des employés doit faire l'objet d'une information préalable des employés et ne peut survenir [qu'en conformité avec la législation et] si cela est nécessaire pour des raisons de sécurité, ou pour d'autres raisons légitimes. En cas d'absence d'un employé, l'employeur devrait prendre les mesures nécessaires et prévoir les procédures appropriées visant à permettre l'accès aux messages électroniques professionnels, uniquement lorsqu'un tel accès est nécessaire d'un point de vue professionnel. Par ailleurs, l'accès doit intervenir de la façon la moins intrusive possible et uniquement après avoir informé l'employé ou les employés concernés.

16.4. En aucun cas le contenu, l'envoi et la réception des messages privés dans le cadre du travail ne peuvent faire l'objet d'une surveillance.

16.5. Lorsqu'un employé quitte son emploi, l'employeur doit prendre des mesures techniques et organisationnelles afin que la messagerie électronique de l'employé soit désactivée automatiquement à son départ. Si le contenu de la messagerie doit être récupéré pour la bonne marche de l'entreprise, l'employeur doit prendre des mesures appropriées afin de récupérer son contenu avant le départ de l'employé et si possible en sa présence.

17. Appareils permettant de géolocaliser les employés

17.1 Si les appareils permettant de localiser les employés peuvent être utilisés dans leur intérêt (par exemple pour déterminer un accident du travail), leur utilisation ne doit pas conduire à leur contrôle permanent ou excessif. Considérant les risques d'atteinte aux droits et aux libertés des personnes que présente l'utilisation de ces appareils, l'employeur devrait prendre toutes les garanties nécessaires à la protection des données à caractère personnel et au respect de la vie privée, y compris les garanties prévues au principe 21. Il doit notamment accorder une attention particulière aux finalités pour lesquelles de tels appareils sont utilisés. En particulier, la surveillance ne doit pas être l'objectif principal poursuivi par l'employeur, mais seulement une conséquence indirecte d'une action nécessaire aux fins de la production, de la sécurité ou de l'organisation du travail de l'établissement.

17.2 Lorsqu'un employé, soit conformément aux instructions de son employeur soit après s'être assuré que l'employeur connaissait au préalable les modalités de cette utilisation et en accord avec ce dernier, utilise des appareils professionnels en dehors de l'entreprise ou de l'institution permettant à l'employeur de le localiser, la collecte et le traitement de ces données à caractère personnel doit être exclusivement limité à la stricte vérification de l'exécution des tâches professionnelles ou des aspects organisationnels.

17.3 L'employeur doit prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux personnes concernées.

18. Données biométriques

18.1 La collecte et le traitement de données biométriques ne devraient être réalisés que lorsqu'ils sont nécessaires à la protection des intérêts légitimes de l'employeur, des employés ou des tiers et uniquement lorsqu'il y a impossibilité d'utiliser d'autres méthodes alternatives de traitement moins intrusives pour la vie privée. Ce traitement doit s'accompagner de garanties appropriées, y compris les garanties prévues au principe 21.

18.2 Le traitement des données biométriques doit être fondé sur des méthodes scientifiquement reconnues et soumis à des exigences strictes de sécurité et de proportionnalité. L'employé devrait avoir le contrôle du traitement de ces données biométriques.

19. Tests psychologiques, analyses et procédures analogues

19.1 Le recours à des tests, à des analyses et à des procédures analogues effectués par des professionnels spécialisés, soumis au secret professionnel et destinés à évaluer le caractère ou la personnalité d'un employé ou d'un candidat à l'emploi ne devraient être permis que s'il est légitime et nécessaire au regard de la catégorie d'activité exercé dans l'emploi.

19.2 Ces tests, analyses et procédures analogues ne devraient pas se faire sans le consentement de l'employé ou du candidat à l'emploi, et en vertu des garanties appropriées

prévues par le droit interne, y compris les garanties prévues au principe 21. Le consentement de l'employé doit être libre, éclairé et sans aucune contrepartie, notamment financière. L'employé ou le candidat à l'emploi devraient être informés au préalable des modalités d'utilisation des résultats de ces tests, analyses ou procédures analogues et, par la suite, de leur contenu.

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

20.1 L'employeur, et lorsque cela est applicable, le sous-traitant, doivent procéder à une analyse de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des employés et concevoir les traitements de données de manière à prévenir ou pour le moins à minimiser les risques d'atteinte à ces droits et libertés fondamentales.

20.2 A moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale, l'accord des représentants des employés devrait être recherché préalablement à l'introduction ou à la modification des TICs lorsque la procédure de consultation mentionnée au principe 14 révèle des risques d'atteinte au regard des droits des employés.

21. Garanties complémentaires

- Pour toutes formes particulières de traitement, établies dans la Partie II de cette Recommandation, l'employeur est tenu de prendre en particulier les garanties suivantes :

- Informer préalablement les employés de la mise à place de tout dispositif de surveillance. L'information fournie doit être mise à jour, et le droit d'information doit s'effectuer conformément au principe 10 de la Recommandation. Les informations doivent inclure la finalité du dispositif, la durée de conservation, l'existence ou non des droits d'accès et de rectification et la façon dont ces droits peuvent être exercés ;

- Prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux employés ;

- Avant l'introduction d'un système de surveillance ou lorsqu'un système existant doit être modifié, les représentants des employés devraient être consultés, conformément aux législations et pratiques nationales. 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, l'accord des représentants doit être assuré ;

- Consulter, conformément à la législation nationale les autorités nationales de contrôle sur les traitements de données à caractère personnel.