**Recommandation CM/Rec(2015)5**

**du Comité des Ministres aux Etats membres**

**sur le traitement des données à caractère personnel dans le cadre de l'emploi**

*(adoptée par le Comité des Ministres le 1er avril 2015,*

*lors de la 1224e réunion des Délégués des Ministres)*

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, ainsi que des avantages qui en découlent ;

Estimant, toutefois, que l'utilisation de méthodes de traitement de données par les employeurs devrait être gouvernée par des principes destinés à réduire 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 (STE n° 108, ci-après la « Convention n° 108 »), ainsi que celles de son Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001 (STE n° 181), et compte tenu de l'intérêt d'appliquer ces principes au secteur de l'emploi ;

Reconnaissant également que les intérêts devant être pris en compte lors de l'élaboration de principes dans le secteur de l'emploi sont individuels ou collectifs, privés ou publics ;

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 l'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 aux principes de 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 les activités qui y sont liées, du fait notamment du recours accru aux technologies de l'information et de la communication (TIC) et de la mondialisation de l'emploi et des services ;

Considérant que ces changements appellent à une révision de la Recommandation Rec(89)2 du Comité des Ministres aux Etats membres 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 cadre de l'emploi ;

Rappelant l'article 8 de la Convention européenne des droits de l'homme (STE n° 5), 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 Comité des Ministres du Conseil de l'Europe aux Etats membres, 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 Rec(97)5 relative à la protection des données médicales et la Recommandation Rec(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) sur la vidéosurveillance des lieux publics de l'Assemblée parlementaire du Conseil de l'Europe, qui sont particulièrement pertinents ;

Rappelant la Charte sociale européenne (STE nº 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 l'annexe de la présente recommandation, qui remplace la Recommandation Rec(89)2 susmentionnée, sont 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 et son annexe sont portées à l'attention des autorités établies conformément à la législation nationale en matière de protection de données et chargées de contrôler l'application de cette législation ;

– de promouvoir 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 sont bien connus, compris et mis en application par tous les intervenants du secteur de l'emploi, y compris les organes représentatifs des employeurs et des employés, et pris en compte dans la conception, le déploiement et l'utilisation des TIC dans ce secteur.

*Annexe à la Recommandation CM/Rec(2015)5*

## Partie I – Principes généraux

### *1. Champ d'application*

1.1. Les principes de la présente recommandation s'appliquent à tout 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 découlant desdits contrats.

### *2. Définitions*

Aux fins de la présente recommandation :

« Données à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») ;

« Traitement de données » 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 ou 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 ;

« 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 enregistrées, traitées, récupérées ou transmises par les systèmes d'information en vue de leur fonctionnement, utilisation, protection ou maintenance ;

« A des fins d'emploi » concerne les rapports entre employeurs et employés relatifs au recrutement, 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 à la gestion efficace d'une organisation, et à 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, autorité publique ou agence, engagée dans un lien d'emploi avec l'employé ou qui envisage d'engager un tel lien avec un candidat à un emploi et qui détient la responsabilité légale de l'entreprise ou de l'établissement ;

« Employé » signifie toute personne concernée engagée dans une relation de travail avec un employeur.

***3. 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 de 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.

***4. Application des principes de traitement des données***

4.1. 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.

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

***5. Collecte et enregistrement des données***

5.1. Les employeurs devraient collecter les données à caractère personnel directement auprès de la personne concernée. Lorsqu'il est nécessaire et licite de traiter des données collectées auprès de tiers, par exemple pour obtenir des références professionnelles, la personne concernée devrait en être préalablement dûment informée.

5.2. 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.

5.3. Les employeurs devraient s'abstenir d'exiger ou de demander à un employé ou à un candidat à l'emploi d'avoir accès à des informations que celui-ci partage avec d'autres en ligne, notamment sur des réseaux sociaux.

5.4. Les données relatives à la santé ne peuvent être collectées qu'aux fins prévues au principe 9 de la présente recommandation.

5.5. 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, et uniquement pour le temps nécessaire à la poursuite des finalités du traitement. Ces données devraient être pertinentes, adéquates et non excessives. Lorsque des données d'évaluation relatives à la productivité ou à la capacité d'un employé 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 les employeurs qu'à de telles fins.

6.2. Les employeurs devraient adopter des politiques de protection des données, des règles et/ou d'autres instruments relatifs à l'usage interne des données à caractère personnel conformément aux principes de la présente recommandation.

6.3. A titre exceptionnel, 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, les employeurs devraient prendre des mesures appropriées pour éviter que ces données ne soient mal interprétées pour cette autre finalité et en informer l'employé. En cas de décision importante concernant l'employé, fondée sur des données ainsi utilisées, celui-ci devrait en être avisé.

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. Toute modification substantielle du traitement devrait être communiquée à la personne concernée.

***7. Communication des données et utilisation des TIC pour la représentation des employés***

7.1. Conformément aux législations et pratiques nationales, ainsi qu'aux conventions collectives, des données à caractère personnel ne peuvent être communiquées aux représentants des employés que si de telles données sont nécessaires pour permettre à ceux-ci de représenter de façon appropriée les intérêts des employés concernés ou 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, visant à définir au préalable des règles transparentes stipulant leur utilisation et garantissant la protection des communications confidentielles, conformément au principe 10.

***8. Communication externe des données***

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

8.2. La communication de données à caractère personnel à des organismes publics à des fins autres que l'accomplissement de leur mission officielle ou à des parties autres que les 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 concernés ou leurs représentants, selon le cas, en sont informés au préalable ;

*b.* avec le consentement exprès, libre et informé de l'employé concerné ;

*c*. si la communication est prévue par le droit interne et notamment lorsqu'elle est nécessaire à l'exécution d'obligations découlant de la loi ou des conventions collectives.

8.3. Les dispositions relatives à la divulgation de données à caractère personnel afin d'assurer la transparence dans le secteur public (le gouvernement et toute autre autorité publique ou organisme), y compris le contrôle de l'utilisation régulière 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.

8.4. Les employeurs devraient prendre les mesures appropriées afin de veiller à ce que seules des données pertinentes, exactes et à jour soient communiquées en externe, à plus forte raison s'agissant des données publiées en ligne et accessibles à un plus large public.

***9. Traitement des données sensibles***

9.1. Le traitement des données sensibles, visé à l'article 6 de la Convention n° 108, n'est permis que dans des cas particuliers, lorsque cela est indispensable pour un recrutement spécifique ou pour l'exécution d'obligations légales dérivant du contrat de travail, dans les limites prescrites par le droit interne et moyennant des garanties appropriées, venant compléter celles de la Convention n° 108 et de la présente recommandation. Les garanties appropriées devraient 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 soumis aux dispositions du principe 18 de la présente recommandation.

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

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

*b.* répondre aux exigences de la médecine préventive ;

*c.* garantir sa réadaptation appropriée au poste de travail ou répondre à toute autre exigence de l'environnement professionnel ;

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

*e.* octroyer des prestations sociales ;

*f.* répondre à une procédure judiciaire.

9.3. Les données génétiques ne peuvent pas faire objet d'un traitement pour déterminer, par exemple, l'aptitude professionnelle d'employés ou de candidats à l'emploi, même avec le consentement de l'intéressé. Le traitement de données génétiques ne peut être permis qu'à titre exceptionnel, par exemple pour éviter une atteinte grave à la santé de la personne concernée ou de tiers, et uniquement lorsque cela est prévu par le droit interne et moyennant des garanties appropriées.

9.4. Les données de santé et – lorsque leur traitement est licite – les données génétiques, ne devraient être collectées qu'auprès de l'employé, lorsque cela est prévu par la loi et moyennant des garanties appropriées.

9.5. 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 ;

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

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

Lorsque ces données sont communiquées à l'employeur, cette communication devrait être faite par une personne dûment habilitée, telle qu'une personne travaillant dans l'administration du personnel, ou ayant des responsabilités dans le secteur 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 et conformément au droit interne.

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

9.7. Les données de santé relatives à des tiers ne devraient en aucune circonstance faire l'objet d'un traitement, à moins que la personne concernée ait donné au préalable son entier consentement, libre, informé et non équivoque, ou que ce traitement soit autorisé par l'autorité de contrôle compétente en matière de protection des données, ou que la collecte des données soit indispensable à l'exécution des obligations légales.

***10. Transparence du traitement***

10.1. Des informations sur les données à caractère personnel détenues par des employeurs devraient être mises à la disposition de l'employé concerné, soit directement, soit par l'intermédiaire de ses représentants, ou être portées à sa connaissance par d'autres moyens appropriés.

10.2. Les employeurs devraient fournir à leurs employés les informations suivantes :

– les catégories de 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 principe 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.

10.3. Une description particulièrement claire et complète des catégories de données à caractère personnel qui peuvent être collectées au moyen de TIC, telle que la vidéosurveillance, et de leur utilisation potentielle, devrait être fournie. Ce principe vaut pour toutes les formes particulières de traitement de données à caractère personnel prévues à la partie II de l'annexe de la présente recommandation.

10.4. Les informations devraient être fournies sous une forme accessible et tenues à jour. Ces informations devraient, en tout état de cause, être fournies avant que l'employé 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'opposition***

11.1. Un employé devrait pouvoir obtenir, à sa demande, à fréquence raisonnable et dans un délai normal, la confirmation d'un traitement de données le 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 principe 10.

11.2. Un employé devrait avoir le droit d'obtenir la rectification, le blocage ou l'effacement de ses données à caractère personnel en cas d'inexactitude et/ou lorsqu'elles sont traitées en violation du droit interne ou des principes énoncés dans la présente recommandation. Il devrait également être autorisé à s'opposer à tout moment au traitement des données à caractère personnel le concernant, à moins que ce traitement soit nécessaire à des fins d'emploi ou 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 des employeurs ou des tiers impliqués. Bien que ces données ne puissent être directement corrigées par l'employé, les évaluations purement subjectives devraient pouvoir être contestées conformément au droit interne.

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

11.5. Un employé devrait également pouvoir obtenir, à sa demande, des informations concernant le raisonnement qui sous-tend le traitement de données dont les résultats lui sont appliqués.

11.6. Des dérogations aux droits auxquels il est fait référence aux paragraphes 10, 11.1, 11.2, 11.4 et 11.5 peuvent être admises lorsqu'elles sont prévues par la loi et constituent une mesure nécessaire, dans une société démocratique, à la protection de la sécurité nationale, à la sûreté 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. En outre, dans le cas d'une enquête interne effectuée par un employeur, l'exercice des droits auxquels il est fait référence aux paragraphes 10 et 11.1 à 11.5 peut être différé jusqu'à la conclusion de cette enquête si cet exercice devait porter préjudice à 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'opposition, ou afin d'exercer ces droits en son nom.

11.9. Des voies de recours devraient être prévues 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 ses données.

***12. Sécurité des données***

12.1. Les employeurs, ou les entités auprès desquelles le traitement de données peut être sous-traité, devraient mettre en œuvre des mesures techniques et organisationnelles appropriées, qui seront mises à jour si cela s'avère nécessaire, en réponse aux examens périodiques d'évaluation des risques et des politiques de sécurité. De telles mesures devraient garantir la sécurité et la confidentialité des données à caractère personnel traitées 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, la diffusion ou la divulgation non autorisées des données.

12.2. Conformément au droit interne, les employeurs devraient garantir de manière adéquate la sécurité des données lors de l'utilisation des TIC pour toute opération de traitement de données à caractère personnel à des fins d'emploi, y compris leur

enregistrement.

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, ainsi que de garder la confidentialité concernant ces mesures.

***13. Conservation des données***

13.1. Les employeurs ne devraient pas traiter des données à caractère personnel pendant une période plus longue que ne le justifient les finalités d'emploi définies au principe 2 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 par l'employeur ou sera retirée par le candidat. Lorsque de telles données sont conservées en vue d'une demande d'emploi ultérieure, l'intéressé devrait en être informé en conséquence et les données devraient être effacées à sa demande.

13.3. 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 cette finalité.

13.4. Les données à caractère personnel traitées aux fins d'une enquête interne réalisée par des employeurs qui n'a entraîné l'adoption d'aucune sanction à l'égard d'un employé 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. Utilisation de l'internet et des communications électroniques sur le lieu de travail***

14.1. Les employeurs devraient éviter de porter des atteintes injustifiées et déraisonnables au droit au respect de la vie privée des employés. Ce principe s'étend à tous les dispositifs techniques et aux TIC utilisés par un employé. Les personnes concernées devraient être convenablement et périodiquement informées en application d'une politique claire en matière de respect de la vie privée, conformément au principe 10 de la présente recommandation. L'information fournie devrait être mise à jour et inclure la finalité du traitement, la durée de conservation des données collectées, la sauvegarde des données de connexion et l'archivage des messages électroniques professionnels.

14.2. En ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel relatif aux pages internet ou intranet consultées par l'employé, il conviendrait de préférence 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 préférence, de manière graduée et par sondages non individuels, en utilisant des données anonymes ou, en quelque sorte, agrégées.

14.3. L'accès par des employeurs aux communications électroniques professionnelles de leurs employés, qui ont été informés au préalable de cette éventualité, ne peut survenir, le cas échéant, que si cela est nécessaire pour des raisons de sécurité ou pour d'autres raisons légitimes. En cas d'absence d'un employé, les employeurs devraient prendre les mesures nécessaires et prévoir les procédures appropriées visant à permettre l'accès aux communications électroniques professionnelles, uniquement lorsqu'un tel accès est nécessaire d'un point de vue professionnel. L'accès devrait intervenir de la façon la moins intrusive possible et uniquement après avoir informé les employés concernés.

14.4. En aucun cas le contenu, l'envoi et la réception de communications électroniques privées dans le cadre du travail ne devraient faire l'objet d'une surveillance.

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

### *15. Systèmes et technologies de l'information pour le contrôle des employés, notamment la vidéosurveillance*

15.1. L'introduction et l'utilisation des systèmes et technologies d'information ayant pour finalité directe et principale le contrôle de l'activité et du comportement des employés ne devraient pas être permises. Lorsque leur introduction et leur utilisation sont nécessaires pour d'autres finalités légitimes, telles que la protection de la production, de la santé, de la sécurité ou la gestion efficace d'une organisation et mènent de façon indirecte à la possibilité de contrôler l'activité des employés, elles devraient être soumises aux garanties complémentaires visées au principe 21, notamment la consultation des représentants des employés.

15.2. Les systèmes et technologies de l'information qui contrôlent l'activité et le comportement des employés de façon indirecte devraient être spécialement conçus et placés de façon à ne pas porter préjudice à leurs droits fondamentaux. L'utilisation de la vidéosurveillance pour le contrôle de lieux ayant trait à la vie intime des employés n'est en aucun cas autorisée.

15.3. En cas de litige ou d'action en justice, les employés devraient, le cas échéant, pouvoir obtenir, si cela est approprié, la copie des enregistrements réalisés, conformément aux dispositions du droit interne. La conservation des enregistrements devrait être limitée dans le temps.

### *16. Appareils permettant de localiser les employés*

16.1. Les appareils permettant de localiser un employé ne devraient être introduits que s'ils s'avèrent nécessaires pour atteindre les finalités légitimes poursuivies par les employeurs et si leur utilisation ne conduit pas à un contrôle permanent des employés. Plus particulièrement, le contrôle ne devrait pas être la finalité principale, mais uniquement une conséquence indirecte de l'action visant la protection de la production, de la santé, de la sécurité ou de la gestion efficace d'une organisation. Considérant les risques d'atteinte aux droits et aux libertés des personnes que présente l'utilisation de ces appareils, les employeurs devraient prendre toutes les garanties nécessaires à la protection des données à caractère personnel et au respect de la vie privée des employés, y compris les garanties prévues au principe 21. Conformément aux règles définies aux principes 4 et 5, les employeurs devraient accorder une attention particulière aux finalités pour lesquelles de tels appareils sont utilisés et aux principes de minimisation et de proportionnalité.

16.2. Les employeurs devraient prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux personnes concernées.

### *17. Mécanismes internes de signalement*

17.1. Lorsque les employeurs sont tenus par la loi ou les règles internes de mettre en œuvre des mécanismes internes de signalement, tels que les numéros d'urgence, ils devraient assurer la protection des données à caractère personnel de toutes les parties concernées. En particulier, les employeurs devraient 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 ne devraient être utilisées qu'aux fins des procédures internes appropriées relatives auxdits signalements, ainsi que prévu par la loi ou pourrait être prévu par des procédures judiciaires ultérieures.

17.2. A titre exceptionnel, les employeurs peuvent permettre le signalement anonyme. Un signalement anonyme ne saurait être l'unique origine d'enquêtes internes, à moins que ce signalement soit dûment circonstancié et concerne de graves infractions au droit interne.

***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 des employeurs, des employés ou des tiers, uniquement lorsqu'il y a impossibilité d'utiliser d'autres méthodes alternatives de traitement moins intrusives pour la vie privée et lorsque le traitement s'accompagne de garanties appropriées, y compris les garanties prévues au principe 21.

18.2. Le traitement des données biométriques devrait être fondé sur des méthodes scientifiquement reconnues et soumis à des exigences strictes de sécurité et de proportionnalité.

***19. Tests psychologiques, analyses et procédures analogues***

19.1. Le recours à des tests psychologiques, à des analyses et à des procédures analogues effectués par des professionnels spécialisés, soumis au secret médical, et destinés à évaluer le caractère ou la personnalité d'un employé ou d'un candidat à l'emploi ne devrait être permis que s'il est légitime et nécessaire au regard de la catégorie d'activité exercée dans l'emploi et si le droit interne prévoit des garanties appropriées.

19.2. L'employé ou le candidat à l'emploi devrait être informé au préalable des modalités d'utilisation des résultats de ces tests, analyses ou procédures analogues et, par la suite, de leur contenu. Les principes 11.1 et 11.2 s'appliquent en conséquence.

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

20.1. Les employeurs, et le cas échéant, les sous-traitants, devraient procéder à une analyse de l'impact potentiel de tout 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 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 TIC lorsque la procédure révèle des risques d'atteinte aux droits et libertés fondamentales des employés.

***21. Garanties complémentaires***

Pour toutes formes particulières de traitement, établies dans la partie II de la présente recommandation, les employeurs devraient respecter en particulier les garanties suivantes :

*a.* informer préalablement les employés de l'introduction des systèmes et technologies d'information permettant le contrôle de leur activité. L'information fournie devrait être mise à jour et prendre en compte le principe 10 de la présente recommandation. Les informations devraient 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 ;

*b.* prendre les mesures internes appropriées concernant le traitement de ces données et les notifier préalablement aux employés ;

*c*. consulter les représentants des employés conformément aux législations et pratiques nationales, avant l'introduction d'un système de surveillance ou lorsqu'un système existant devrait être modifié. Lorsque la procédure de consultation révèle une

possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine d'un employé, l'accord des représentants devrait être recherché ;

*d.* consulter, conformément à la législation nationale, les autorités nationales de contrôle sur les traitements de données à caractère personnel.

---

## Documents liés

**Réunions**

- 1224e réunion des Délégués des Ministres / 1 avril 2015

**Documents connexes**

- CM/Del/Dec(2015)1224/5.1F / 7 avril 2015
- CM(2015)32addfinalF / 1 avril 2015