COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, le 30 août 2011 T-PD-BUR(2011)07 prov2 FR

LE BUREAU DU 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-BUR)

Projet de recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi [1]

[1] Les changements proposés au texte de la Recommandation (89)2 sont en caractères visibles.

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, notamment automatisé, 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 au respect de la vie privée et à la protection des 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, 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 la nécessité d'adapter ces dispositions 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 processus de production liés, du fait notamment du recours aux technologies de l'information et de la communication et de la globalisation des activités et des services ;
[EM[2] : cela concerne aussi bien le monde du travail public que privé]

Considérant que ces changements appellent à une révision de la Recommandation N° R (89) 2 sur la protection des données à caractè re 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 »[3] 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

[2] EM signifie « exposé des motifs » et indique que des informations supplémentaires seront apportées dans l'exposé des motifs de la Recommandation.
[3] "Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance".

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 du 18 octobre 1961, et en particulier ses articles 1.2 et 6, 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’interprèté 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 s usmentionnée, soient reflétés dans la mise en oeuvre des législations nationales relatives à la protection des données dans le secteur de l'emploi, ainsi que dans d'autres branches du droit portant sur l'utilisation de 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 ;

- 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

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.

Ces principes s'appliquent au traitement automatisé de données à caractère personnel ainsi qu'aux autres informations sur les employés détenues par les employeurs dans la mesure où ces informations sont nécessaires pour rendre intelligibles le traitement automatisé de données ou pour prendre des décisions impactant de façon significative les droits de la personne concernée. (EM: De même, ces principes s’appliquent, s’il y a lieu, aux données à caractère personnel relatives à des personnes extérieures au lieu de travail traitées à des fins de sécurité du travail, ainsi qu’aux organisations syndicales.)

Un traitement de données à caractère personnel, qu’il soit en partie ou totalement automatisé, ne devrait pas être effectué par un employeur dans le but d'échapper aux dispositions de la présente recommandation.

1.2. Nonobstant le principe énoncé au deuxième alinéa du paragraphe 1.1, un Etat membre peut étendre les principes énoncés dans la présente recommandation à tous les traitements non-automatisés.

1.3. Aux fins de la présente recommandation :

- «données à caractère personnel» signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée »). Une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais ou des activités déraisonnables. (EM : applicable par analogie aux associations professionnelles)

– «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. (EM : concerne également les données traitées après la fin du contrat de travail)

1.4. Sauf législations nationales contraires, les principes de la présente recommandation s'appliquent, dans les cas appropriés, 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. (EM : détailler les systèmes d'information et de communication, données génétiques, données sensibles)

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

Le respect des droits de l'homme, de la dignité humaine et des libertés fondamentales, notamment du droit à la vie privée , du droit à la protection des données à caractère personnel, de l'interdiction de la discrimination devraient être garantis 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. Les systèmes et technologies d'information utilisés pour la collecte et le traitement de données à caractère personnel à des fins d'emploi devraient être configurés, le cas échéant certifiés, en vue de réduire au minimum l'utilisation et la conservation des données à caractère personnel, ainsi que de limiter l'utilisation de données permettant une identification directe au strict nécessaire visant à atteindre les objectifs propres à chaque situation. (EM : spécifier que les outils et les dispositifs sont couverts par la notion de systèmes et technologies d'information - référence à 3.3)

3.2. L'employeur devrait 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. *Information et consultation des employés*

4.1. 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, ne devraient [par principe] pas être autorisées lorsqu’elles conduisent à une surveillance permanente des personnes [à l’exception de l’indisponibilité de mesures alternatives qui soient moins intrusives, et pour autant que des garanties appropriées existent].

[EM : sans préjudice des mesures liées aux procédures judiciaires fondées de défense. Le recours à des systèmes et technologies d’information, tels que les systèmes de vidéosurveillance sur le lieu de travail et de géolocalisation, devrait être limité uniquement à des exigences organisationnelles et/ou de production, ou à des fins de sécurité au travail. Ces dispositifs ne sont possibles que s’ils sont légitimes, nécessaires et encadrés de garanties appropriées. Ils ne devraient pas avoir pour but la surveillance délibérée, systématique et permanente de la qualité et de la quantité de travail individuel sur le lieu de travail, ainsi que le contrôle à distance du comportement ou de la position des employés.]

4.2. Dans les cas d'introduction, de modification et de fonctionnement de systèmes et technologies d’information pour la collecte et le traitement des 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, devraient être préalablement informés ou consultés. [EM : traiter des outils également couverts par les systèmes et technologies d’information]

4.3. L’employeur devrait adopter des mesures appropriées pour évaluer l’impact d’éventuels traitements de données et qui peuvent présenter des risques d’atteintes spécifiques 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 invasive 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 4.2 révèle une possibilité d’atteinte, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationales. (EM : pour les entreprises de petites tailles, il s’agit des employés eux-mêmes et non de représentants)

5. *Collecte des données et formes particulières de traitement ou d’informations*

5.1. Les données à caractère personnel devraient en principe être collectées 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.

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. 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 à caractère personnel devraient être recueillies uniquement auprès de l'individu concerné. Sous réserve des dispositions du droit interne, des sources externes, dont celles en provenance de sociétés de conseil ou de réseaux sociaux dédiés au développement de relations professionnelles, ne

peuvent être consultées que si la personne concernée y a consenti ou si elle a été informée au préalable de cette possibilité. Le profilage de l'intéressé basé sur la collecte occulte de données provenant de moteurs de recherche devrait [par principe] être interdit. L'employeur ne devrait pas inciter l'intéressé à lui fournir ou lui permettre l'accès aux données médicales conservées par des tiers. (EM : souligner la valeur ajoutée de cette Recommandation concernant les données médicales électroniques / Ref à la Recommandation (97)5. Définir le profilage)

Il conviendrait en tout état de cause, de 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.

5.4. Le recours à des tests, à des analyses et à des procédures analogues destinés à évaluer le caractère ou la personnalité d'une personne ne devrait pas se faire sans son consentement, ou à moins que d'autres garanties appropriées ne soient prévues par le droit interne. La personne concernée devrait pouvoir, si elle le désire, connaître au préalable les modalités d'utilisation des résultats de ces tests, analyses ou procédures analogues et, par la suite, leur contenu. (EM : aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement de ces tests, analyses ou procédures analogues. L'établissement du profil du candidat ou de l'employé doit être basé sur des données objectives et en aucun cas révéler les données relatives à la santé de la personne. Ces tests doivent être pertinents et se fonder sur des méthodes scientifiquement reconnues. S'agissant de l'information sur le contenu, il est admissible de reporter cette information au titre d'intérêts légitimes, y compris ceux de l'employeur)

5.5. Le traitement des données biométriques visant à identifier ou authentifier les personnes ne devrait être permis que lorsqu'il est nécessaire à la protection des intérêts légitimes de l'employeur, de l'employé ou de tiers et devrait se fonder sur des méthodes scientifiquement reconnues qui garantissent de façon appropriée la sécurité des données. (EM : définir des intérêts légitimes).

5.6. Eu égard à 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 suivantes :

- la configuration de systèmes ou l'utilisation de filtres qui permettent d'empêcher, selon le cas, certaines opérations (EM : comme téléverser ou télécharger des contenus précis) ;

- l'identification de catégories de sites jugés comme corrélés ou non au travail de l'employé ;

- 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 (EM : par exemple, par unité de production).

Les personnes concernées devraient être convenablement informées, conformément aux principes 4 et 12.

Si l'employé utilise, conformément à l'autorisation donnée par son employeur, des appareils susceptibles de signaler l'endroit où il se trouve en dehors de ses heures de travail, il

conviendrait de permettre d'empêcher que ces données ne soient utilisées et de les effacer automatiquement le plus vite possible.

Il conviendrait de définir des procédures internes relatives au traitement de ces données en les portant préalablement à la connaissance des intéressés. (EM : procédures relatives aux politiques de contrôle – également valables dans le cadre d'autres type de traitements ?)

5.7. L'employeur devrait prendre les mesures nécessaires et prévoir les procédures visant à permettre en cas d'absence de l'employé l'accès aux messages professionnels, lorsque ceci est indispensable au fonctionnement du service et après en avoir informé l'employé. L'accès aux messages personnels de l'employé ne peuvent être permis.
(EM : structure : surveillance des employés ?
Si possible, il serait préférable d'attribuer aux employés des adresses de courrier électronique qui soient directement rattachables à des fonctions plutôt qu'à des personnes.
Il conviendrait également de fournir des instructions afin qu'en l'absence d'un employé, le système de messagerie électronique signale l'absence temporaire de l'employé et communique automatiquement les coordonnées d'un autre contact utile.
Afin d'informer le destinataire sur l'utilisation à des fins exclusivement professionnelles du compte de messagerie électronique, un avertissement adéquat devrait figurer dans les messages envoyés par l'employé).

6. *Enregistrement des données*

6.1. L'enregistrement de données à caractère personnel n'est possible que si les données ont été collectées conformément aux règles définies aux principes 4.1 et 5 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.

6.2. Les données enregistrées devraient être exactes, mises à jour si nécessaire, et reproduire fidèlement la situation de l'employé. Elles ne devraient pas être enregistrées ou codées d'une manière qui puisse porter atteinte aux droits de l'employé en permettant de le caractériser ou d'établir son profil sans qu'il en ait connaissance.

Si l'utilisation des données biométriques est permise aux termes du principe 5.5., elles ne devraient pas, en principe, être enregistrées dans une base de données, la préférence devant être accordée, selon les cas, à des systèmes d'identification ou d'authentification biométrique basés sur des supports mis à la disposition exclusive de l'intéressé. (EM : préciser quand un tel enregistrement est possible).

6.3. Lorsque des données appréciatives relatives à la productivité ou à la potentialité des employés sont enregistrées, elles devraient être fondées sur des évaluations équitables et loyales. (EM: elles ne doivent pas être insultantes dans la manière dont elles sont formulées).

7. *Utilisation interne des données*

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

Dans le respect des principes de pertinence et d'exactitude, notamment eu égard à des entreprises de grande dimension ou dispersées sur le territoire, l'accès à certaines données à caractère personnel pourrait être facilité sur les réseaux de communication interne afin que la prestation de travail soit exécutée avec davantage de célérité et pour faciliter l'interaction avec les autres employés. (EM : contexte de large échelle en matière de données

d'identification : outils intranet par exemple tels que : téléphone, email, photo avec consentement seulement)

7.2. Lorsque des données doivent être traitées à des fins d'emploi autres que celles pour lesquelles elles ont été initialement collectées, des mesures appropriées devraient être prises 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. (EM : donner des exemples concrets).

7.3. Les dispositions du principe 7.2 s'appliquent à la mise en relation de fichiers contenant des données à caractère personnel collectées et enregistrées à des fins d'emploi.

7.4. Sans préjudice des dispositions du principe 9, 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. (EM : conformément au droit applicable et si jugé approprié par les autorités de protection des données).

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

8.1. 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.

8.2. L'utilisation de systèmes et technologies d'information pour des communications à caractère syndical devrait faire l'objet 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. (EM : le type d'accord n'est pas déterminé par les autorités de protection des données)

9. *Communication externe et transmission des données*

9.1. 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.

9.2. 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. (EM : donner d'autres exemples)

9.3. 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.
(EM : le rôle du consentement dans certains cas précis ne peut être négligé. Illustrer par des exemples tels que l'échange de CV. Les obligations peuvent concerner la prévoyance et la sécurité sociale des les employés, ou viser l'optimisation de l'affectation des ressources humaines.)

9.4. Dans le secteur public en particulier, la loi devrait permettre de concilier le droit au respect de la vie privée et à la protection des données à caractère personnel avec les implications liées à la transparence ou au contrôle de l'utilisation de ressources et de fonds publics en permettant l'identification de catégories professionnelles ou de profils pour lesquels certaines obligations de publicité existent, ainsi que le type de d'informations qui peuvent être rendues publiques de façon homogène, en considérant notamment la possibilité de faciliter l'identification au moyen des moteurs de recherche externes.

9.5. Lorsque les fonctions professionnelles impliquent des relations constantes avec le public ou lorsque cela est nécessaire afin de satisfaire les exigences de transparence à l'égard des usagers, des consommateurs et des citoyens, des mesures et des garanties appropriées peuvent être adoptées pour rendre directement ou indirectement identifiable l'employé concerné. (EM : il est à cette fin possible d'avoir recours à un code d'identification attribué à l'employé ou une autre référence personnelle.)

10. Catégories particulières de données

10.1. Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, les données relatives à la vie sexuelle ou à des condamnations pénales, visées à l'article 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ne devraient être collectées et traitées que dans des cas particuliers, lorsque cela est indispensable au recrutement ou à l'exécution d'obligations légales dérivant du contrat de travail dans les limites prévues par le droit interne et conformément aux garanties appropriées y figurant. En l'absence de telles garanties, ces données ne devraient être collectées et traitées qu'avec le consentement exprès des employés**,** et à condition que cela soit dans leur intérêt.
(EM: ceci vise également les systèmes de pension et d'assurance maladie négociés par les employeurs ou les organisations syndicales).

10.2. 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 (EM : définir les prestations sociales)

d. répondre à une procédure judiciaire.

En principe, il devrait être interdit de collecter et de traiter des 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. Des dérogations exceptionnelles pourraient être prévues dans les seules limites prévues par le

droit interne et en présence de garanties appropriées et documentées qui devraient également prévoir une participation préalable des autorités de contrôle, uniquement afin d'adopter, à la demande de l'employé, les mesures nécessaires à son état de santé, ses conditions de sécurité ou de travail.
(EM : conformément à la recommandation (97)5, un tel traitement ne peut être autorisé que pour raisons de santé et plus particulièrement pour éviter toute atteinte sérieuse à la santé de la personne concernée ou de tiers).

10.3. 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.

10.4. 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.

10.5. 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.

10.6. 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.

10.7. 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. (EM : fournir des exemples de traitement de données sur la santé relatives à des tiers, comme celles des membres de la famille en vue de l'attribution de prestations spécifiques).

11. *Transparence du traitement*

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

Ces informations devraient spécifier les principales finalités du traitement de ces données, le type de données traitées, les catégories de personnes ou d'organes auxquels les données sont régulièrement communiquées, les finalités et la base juridique de cette communication.

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,. Une description semblable devrait être fournie concernant l'emploi de technologies biométriques et de Radio Frequency Identification (RFID), l'éventuelle utilisation de codes d'identification personnels, ainsi qu'au regard du rôle des administrateurs de système dans le traitement des données.

11.2. Ces informations devraient également faire mention des droits de l'employé au regard de ses données, tels qu'ils sont prévus au principe 12 de la présente recommandation, ainsi que des modalités d'exercice des droits.

11.3. Les informations indiquées aux termes du paragraphe précédent 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. (EM : illustrer les activités ou comportements concernés).

12. *Droit d'accès et de rectification*

12.1. Tout employé devrait pouvoir avoir accès, sur demande, à toutes les données à caractère personnel le concernant détenues par son employeur, et obtenir, le cas échéant, la rectification ou l'effacement de telles données lorsque ces dernières sont détenues en contravention des principes posés dans la présente recommandation, notamment en cas d'inexactitude. Il devrait également se voir reconnaître le droit de connaître toutes les informations disponibles ainsi que leur origine, les parties/tiers auxquelles les données ont été ou sont susceptibles d'être communiquées, ainsi que la logique qui sous-tend le traitement automatisé.

Á 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.
(EM : politique générale justifiant des traitements de contrôle).

12.2. 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 5.3., 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 pas directement, les appréciations purement subjectives devraient pouvoir être contestées selon les modalités prévues par le droit interne. (EM : report, à titre temporaire, du droit d'accès en raison de la procédure de défense).

12.3. Dans le cas d'une enquête interne effectuée par l'employeur, l'exercice des droits mentionnés au principe 12.1 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. (EM : communication des résultats de l'enquête interne à un tiers : référence aux conditions du principe 9.2, visant à éclairer les notions de 'circonstancié' et 'violations graves' et référence à l'avis 1/2006 du groupe de travail de l'article 29 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière).

12.4. Lorsqu'une décision découlant d'un traitement automatisé des données détenues par l'employeur est opposée à l'employé, ce dernier devrait avoir le droit de s'assurer que ces données ont été licitement traitées.

12.5. 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.

12.6. 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.

13. Sécurité des données

13.1. Les employeurs ou les entreprises auprès desquelles les données peuvent être sous-traitées devraient 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 tout accès, utilisation, communication ou modification non autorisés. (EM : les employeurs doivent disposer d'un temps d'adaptation / en lien avec principe 2.3 / référence à l'article 17.3 de la Directive 95 /46 EC sur sous-traitant).

13.2. 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.

14. Conservation des données

14.1. 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.

14.2. 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.

14.3. 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 une période raisonnable.

14.4. Les données à caractère personnel traitées au 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 devraient, en principe, être effacées dans les meilleurs délais, sans préjudice de l'exercice du droit d'accès jusqu'à ce qu'elles soient effacées.