COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, September / septembre 2011 T-PD-BUR(2011) 21MOS

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

LE BUREAU DU COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL [STE n°108]

(T-PD-BUR)

Compilation of comments received on the draft Recommendation on the protection of personal data used for employment purposes

Compilation des commentaires reçus sur le projet de Recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi

Secretariat document prepared by
The Directorate General of Human Rights and Legal Affairs

Document préparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

INDEX / TABLE DES MATIERES

T-PD DELEGATIONS

COUNCIL OF EUROPE COMMITTEES

T-PD DELEGATIONS

REPUBLIC OF CYPRUS / CHYPRE

With regard to the "**Draft Recommendation on the protection of personal data used for employment purposes"** our Office is content to see that most of the suggestions we submitted in February 2011 have been integrated in this draft.
We are convinced that this Recommendation, in conjunction with the Explanatory Memorandum will prove to be a very valuable and important tool both for employees and employers, as well as to trade unions. In the light of the above we have no additional comments on the present draft.

FRANCE

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

Voir mes précédentes propositions pour la rédaction du titre.

[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 ;

1

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 ainsi que dans les ~~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 assurer ~~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 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 :

Mis en forme : Couleur de police : Couleur personnalisée(RVB(148;54;52))

Mis en forme : Couleur de police : Couleur personnalisée(RVB(23;54;93))

Mis en forme : Couleur de police : Couleur personnalisée(RVB(148;54;52))

[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".

- 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 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.)**

Commentaires : Le commentaire « EM » semble élargir l'application des princlpes à des personnes extérieures. Cet élargissement ne devrait-il pas figurer plutôt dans le texte de l'annexe. Je propose de le reprendre dans le corps du texte .
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 (**de quoi ? du contrat ? de l'entreprise ? il faudrait le préciser.)** , y compris pour l'exécution des ~~les~~ obligations découlant de la loi ou de conventions collectives, ainsi que la planification et l'organisation du travail.**(cette fin de phrase depuis « ainsi que » est rattachée à quoi ? à la gestion ou aux rapports entre employés/ employeurs ? la rédaction ne sera pas la m^me (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* *Cet intitulé n'est pas tout à fait compréhensible en français.*

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 nécessaire *(ce qualificatif vient préciser « minimum » terme qui ,en soi , et pour l'application des teXtes de protection des données n'a pas beaucoup de sens)* l'utilisation et la conservation des données à caractère personnel, et afin de ~~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 *(question rédactionnelle : « pouvoir »se rattache à « devrait »ou à « visant à » ?la rédaction ne sera pas alors la m^me)* 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. ***(on ne voit pas à quoi fait référence la fin de la phrase depuis « et »)***

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*(en français, « éventuels »n'est pas clair ; cela fait référence à quoi ? à des traitements envisagés ?)* 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~~ les 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 <u>et formes particulières de traitement ou d'informations</u>*

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 **professionnelle** 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 issues ~~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.*(la phrase pourrait s'arrêter à déloyale. Quelle est la valeur ajoutée par « 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. En principe, le traitement de ces données (EM : définir des intérêts légitimes).

5.6. Eu égard à l'éventuel traitement de données à caractère personnel concernant les consultations effectuées par l'employé de pages Internet ou Intranet ~~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 consultations effectuées ~~aux données à caractère personnel,~~ en procédant ~~moyennant~~ dans un premier temps à 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 par exemple par l'intermédiaire de chartes informatiques internes.

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 mettre en place les procédures nécessaires pour empecher que ces données ne soient utilisées et prévoir leur effacement automatique dans les plus brefs délais. ~~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 à ce que les données ne soient pas traitées ultérieurement de manière incompatible avec la finalité initiale. ~~au respect du principe de finalité 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 et 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. ***Ce paragraphe dans son ensemble n'est pas clair en français.J'essaye de trouver une rédaction alternative*****. 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~~ 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 préventive 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 et en veillant à la stricte nécessité des données collectées (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). ***Je propose de rajouter l'idée que la collecte de ces données est possible mais qu'elle doit être limitée à ce qui est strictement nécessaire (par ex dans le cas de l'attribution d'une aide pour enfant handicapé, la seule connaissance de l'existence d'un handicap peut suffire , l'employeur n'a pas nécessairement besoin de connaitre la nature du handicap.*** **)**

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 ainsi que ~~Une description semblable devrait être fournie~~ dans les cas de ~~concernant~~ l'emploi de technologies biométriques et de Radio Frequency Identification (RFID), comme lors de l'éventuelle utilisation de codes d'identification personnels. Cette information devrait aussi être dispensée concernant le 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 **notamment en cas d'inexactitude ou** 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 ainsi que les sources 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 effectué dans les meilleurs délais ~~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 à d'appréciation, 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, le besoin de l'employeur ou de tiers de se défendre étant temporairement écarté ; même si l'employeur ne les rectifie 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 **notamment de traçabilité des accès** ***(cet aspect de traçabilité est une question importante en matière de protection des données ; il e semble qu'on pourrait y faire référence ici ou au moins dans l'EM)*** **et mises à jour pour prendre en compte les évolutions technologiques ~~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 du fait 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 leur effacement ~~ce qu'elles soient effacées.~~

IRELAND / IRLANDE

General Comments

The document comprehensively deals with the issue of processing personal data for employment purposes. It is welcome that issues arising in the context of ICT, e.g. monitoring internet usage by employees, are addressed in the draft recommendations.

The recommendations deal with the collection and processing (paragraph 5), storage (paragraph 6), use (paragraph 7) and conservation of data (paragraph 14). However, the issue of whether and under what circumstances data should be destroyed is not explicitly addressed in the current draft. Paragraph 14 touches on the issue by reference to conservation of data and does refer to deletion of data of unsuccessful job applicants. No specific reference however is made to current employees and their rights in relation to stored data once they have left employment.

Specific Comments
Recommendation
Recital 9
It is suggested that the word 'impose' should be replaced with 'necessitate' or 'require'.

Recital 10
It is suggested that the phrase 'which are fully topical and relevant' should be replaced with 'which remain appropriate and relevant'.

Appendix to Recommendation
Paragraph 2

We consider that it is not necessary to justify why respect for human rights, etc. should be safeguarded in the processing of personal data for employment purposes. We would therefore suggest that the phrase 'notably to allow to employees the free development of their personality and to foster possibilities of individual and social relationship on the workplace' should be deleted.

Paragraph 3.1
It is not clear who is intended to certify the information and technology systems referred to in this paragraph.

Paragraph 3.3
It is suggested that 'concerned' should be after 'entity'.

Paragraph 4.1
It is suggested that the word 'localisation' should be replaced with 'location'.

Paragraph 5.3
It is difficult to see how this recommendation could be enforced. Moreover, it could be argued that if an individual voluntarily posts information about themselves on a social or professional networking site, they must be aware that the information will be available to third parties including potential employers. Thus, the recommendation could be considered overly restrictive. It does however need to be recognised, that in the absence of a "right to be forgotten" there is a danger that previous behaviour by a younger self recorded by social media sites could have adverse implications for employment. It should be considered whether this recommendation is the appropriate forum for dealing with that risk.

Paragraph 5.4
We consider that individuals should in principle be informed in advance of the use that will be made of the results of tests, analyses and similar procedures designed to assess the character or personality of the individual.

Paragraph 5.6
Are the penultimate and final subparagraphs contradictory? It is stated in the penultimate subparagraph that 'arrangements should be made so that data relating to such whereabouts are not used' whereas in the final paragraph, it is stated that 'Appropriate internal procedures relating to processing of that data should be established and notified …'.

Paragraph 5.7
There is an assertion here that access to personal e-mails of the employee should "never be permitted". This would appear to be too extreme - could there not be circumstances where access could reasonably be required?

Paragraph 6.2
By providing an inherent link to an individual's identity, biometric information could potentially be used for numerous different purposes. Thus, the recommendation that as a rule biometric data should not be stored in databases goes some way to mitigating the potential for function creep.

Paragraph 12.1

It is not clear what is meant by referring to the introduction of "general *preventative* procedures to ensure that there is an adequate and prompt response " where employees seek access to the information about them which is stored by their employer.

Paragraphs 11.3, 14.3 and 14.4
It is not clear what is meant by the phrase " in due time"; it is suggested that it should be replaced with “as soon as practicable.

ITALY / ITALIE

I would like to point your attention only on the par. 4.1, proponing to eliminate the following sentence “[*except where no alternative means which are less intrusive are available and where appropriate safeguards exist*]”.

This paragraph seems to be in contrast with some national laws (as the Italian one) providing for a strict prohibition to permanent monitoring of employees and it creates the “inopportune” effect that the T-PD (a group of expert in data protection) ratifies for the first time the possibility to monitor employees.

PORTUGAL

Having analyzed the text of the Draft Recommendation on the protection of personal data used for employment purposes (T-PD-BUR (2011) 07 prov 2 – Strasburg, 30 June 2011), Portugal would like to stress that despite being a good starting point, this text is still far from definitive in a number of aspects.

Our position contains General Remarks and Specific Remarks. At the end you may find a Final Note concerning Portugal’s approach to the revision of the Recommendation.

General Remarks

Scope of the Recommendation

Portugal considers that the Recommendation should be addressed to both private and public sectors. Differences in processing personal data in the private and public sectors should however be taken into consideration. This option is to be made within the text of the Recommendation itself; further explanations should be included in the Explanatory Report.

The explanatory report only should be used to facilitate the interpretation or detail content of the text of the Recommendation. Draft options not adopted should not be included unless they are necessary to understand the content of the Recommendation.

Secrecy of collected personal data

Several questions arise when reading paragraph 5.3: is the secret collection of personal data admissible? If so, it is to be secret for whom?
Portugal admits that a few exceptions should be admissible, as for instance the collection of confidential data about candidates applying to certain specific high specialized sensitive jobs.

Surveillance of emails and access to websites

The surveillance of emails or access to websites should be regarded as an exception that must be fully justified and comply with personal data protection rules. It should also be limited, as a general rule, to knowing which IP address were accessed.

It is advisable that the access to the content of emails without the knowledge of the employee or against her or his will can only take place within the framework of a criminal procedure.

Specific remarks

We suggest the following new paragraph to be added:

"The principles of this Recommendation apply to all employees and employers (including public employers such as National, Regional or Local Administrations), as well as to the associations that represent their interests, such as trade unions and employers associations."

Amendment to paragraph 4.3

In par. 4.3, the following should be added: "The agreement between employees and employers representatives (…)".

Consequently the pertinent part of that paragraph would read:
"The agreement of employees' and employers' representatives should be sought before the introduction or adaptation of such information systems and technologies where the information or consultation procedure referred to in principle 4.2 reveals such risks unless domestic law or practice provides other appropriate safeguards."

Amendment to paragraph 5.7

As Portugal believes that the current draft is too restrictive, we would suggest the following:
"Access to personal emails shall not be permitted, except when authorized by law".

Suggestion for paragraph 10.2.d

The present draft is:
"10.2: "An employee or job applicant may only be asked questions concerning his or her state of health and be medically examined in order:"
"d. to satisfy judicial procedures".

We suggest the elimination of 10.2.d.

Personal data regarding the employee that was neither supplied by her or him nor obtained previously to the judicial procedure from other lawful source will be obtained according to applicable procedure law rules.

This should be left to the national laws.

Final Notes

Portugal considers that the Draft Recommendation is highly detailed in some aspects, going far beyond what a Recommendation should be.

We believe this text to enter in some detailed approach that a Recommendation is not supposed to do and should therefore be left to national legal instruments.

Attached to this note, you will find the comments of Portuguese trade unions corporations and employers 'corporations, and also the opinion of the Portuguese DPA, which should be regarded as their own point of views and not as the expression of the Portuguese State opinions.

REPUBLIC OF LITHUANIA / LITUANIE

COMMENTS ON THE DRAFT RECOMMENDATION ON THE PROTECTION OF PERSONAL DATA USED FOR EMPLOYMENT PURPOSES

1. Taking into account that video surveillance heavily affects the psychological state of the data subject it could be reasonable to enlarge Article 4.1. as follows:
4.1. Technologies which enable to establish conditions under which the person might be monitored permanently, such as video surveillance may be used for the purpose of ensuring safety and protection of life or health of the employee only in these cases when other ways or measures are insufficient for the achievement of the above mentioned purposes unless they are overridden by the interests of the data subject.

2. We would like to propose small changes of the Article 4.2. as follows:
4.2. In case of the introduction, adaptation **and operation of information systems and technologies** for the collection and processing of **personal data necessary for requirements relating to production or safety or work organisation, employees or their representatives,** in accordance with domestic law or practice and, where appropriate, in accordance with the relevant collective agreements, should, in advance, be fully informed **and** consulted**. [EM: tools also covered by information systems and technologies]**

Supprimé : or

3. Because information about lifestyle as well as medical information might be used for indirect discrimination of the person in the labour market profiling in some cases could be limited. The proposal is to change Article 5.3 as follows:
5.3. In the course of a recruitment **or promotion** procedure, the data collected should be limited to such as are necessary to evaluate the suitability of **the persons concerned** and their career potential.

In the course of **a recruitment**, personal data should be obtained solely from the individual concerned. Subject to provisions of domestic law, **external** sources, **including those from consultancies or social networks for the development of professional relationships,** may only be consulted with the consent o**f the individual concerned or if he or she** has been informed in advance of this possibility. **Profiling of the person concerned based on the secret collection of data from search engines should [in principle] be prohibited. An employer should not persuade the person concerned to provide or to enable access to any medical information and/or information about his or her lifestyle held by him or her or third parties.**

[EM: added value of this Recommendation concerning electronic medical data / Ref recommendation (97)5 – explain profiling]

In any event, appropriate measures should be taken so that also in the case of data readily accessible in electronic communications networks available to the public, only relevant, accurate and up-to-date data are used, thus also avoiding misinterpretation or unfair processing of that data viewed in the light of the context of its origin.

4. The proposal is to change Article 10.2 as follows:

10.2. An employee or job applicant may only be asked questions concerning his or her state of health and/or be medically examined in order:

a. to determine the**ir** suitability for the present or future employment;

b. to fulfil the requirements of preventive medicine;

c. to allow social benefits to be granted**; or [EM: explain social benefits]**

d. **to satisfy judicial procedures.**

SWEDEN / SUÈDE

Draft Recommendation on the protection of personal data used for employment purposes[4]

Sweden appreciates the opportunity to comment upon the Draft Recommendation on the protection of personal data used for employment purposes. Please find below our comments.

General comments and remarks

- In order for the Recommendation to remain valid despite the constant development of new technologies the Recommendation should not be too detailed and, to the extent possible, neutral as regards the technology. The current draft is still quite detailed and certain provisions still has too much focus on specific technologies (for example e-mails, Internet and intranets). Hence,

[4] Changes proposed to the existing text of Recommendation (89)2 are highlighted.

there is a risk that the Recommendation quite quickly will be outdated. It should be considered to move such provisions to the Explanatory Memorandum.

- Some provisions imposes too far-reaching obligations on employers, for example as regards employee's' use of the employer's equipment.

- In some articles the consent of the employee is required. To use the employee's consent as a legal basis for processing may be problematic as the employee is often in a position of dependence in relation to the employer. It may, thus, be put in question to what extent an employee may provide a freely given consent. It should therefore be considered to require another legal basis such as the weighing of the interest between the employer's need to process data on one hand and respect for the employee's privacy on the other hand (as provided for in article 7 f of directive 95/46/EC).

Sweden would furthermore like to propose specific changes of the wording in some of the articles below.

DRAFT RECOMMENDATION CM/REC(2011)… OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE PROTECTION OF PERSONAL DATA USED FOR EMPLOYMENT PURPOSES.

(Adopted by the Committee of Ministers on … 2011
at the … meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity among its members;

Aware of the increasing use of **new technologies and means of electronic communication** in the relations between employers and employees, and the corresponding advantages thereof;

Believing, however, that the use of **data processing methods, in particular automatic processing,** by employers should be guided by principles which are designed to minimise any risks which such methods could possibly pose for the rights and fundamental freedoms of employees, in particular their rights to privacy **and protection of personal data**;

Bearing in mind in this regard the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 **and of its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows of 8 November 2001**, and the desirability of adapting them to the particular requirements of the employment sector;

Recognising also that the interests to be borne in mind when elaborating principles for the employment sector are of an individual as well as collective natureand recognising the social partner's right to freely negotiate according to article 6 of the European Social Charter of 18 October 1961.

Aware of the different traditions which exist in the member states in regard to regulation of different aspects of employer-employee relations, regulation by law being only one method of regulation; collective agreements, general legal principles and case-law constitute others.

Justification:

As a general remark to the use of expressions such as “domestic law”, “regulated by law”, “legal obligations” etc throughout the Recommendation Sweden would like to draw attention to the fact that labour market issues in Sweden, according to long-standing tradition, mainly are regulated by the parties on the labour market through collective agreements. Moreover, case-law from the Labour Court is of great importance since it often delivers generally applicable rulings with guiding principles and establishes general legal principles.

Therefore, where the Recommendation says domestic law, laid down by law, lawfully, regulated etc this will in Sweden be interpreted as also covering collective agreements, general legal principles and guiding case-law. This should be described in the Explanatory Memorandum.

The Swedish system has in fact been tried by the ECHR in a decision as to the admissibility of an application (no 46210/99 by Inga-Lill WRETLUND).

Although the obligation in question (to submit to drug testing as was the case in question) did not follow from legislation, the ECHR observed that labour market issues are, according to long-standing tradition in Sweden, mainly regulated by the parties on the labour market through collective agreements. The ECHR noted that the employer's right to manage and organise the work is a principle agreed upon by those parties and the Labour Court had established that this right constitutes a general legal principle. According to the Labour Court's case-law, the employer may have a right to carry out control measures as part of the right to manage and organise the work.

The Labour Court had concluded, before the events of the present case, that such control measures could include drug and alcohol tests. Also in the judgment in the present case, the Labour Court considered that the tests in question were naturally connected with activities of the company in question and that the right to order employees to undergo such tests therefore could be seen as part of the company's right to manage and organise the work according to the central collective agreement.

In these circumstances, the ECHR was satisfied that the measure challenged by the applicant had a sufficient basis in Swedish law and thus was “in accordance with the law” within the meaning of Article 8 § 2 of the Convention.

Aware of the changes which have occurred internationally in the working world and related production processes; notably due to the use of information and communication technologies and of the globalisation of activities and services;

[EM[5]: private and public employment]

Considering that such changes impose a revision of Recommendation No. 89 (2) on the protection of personal data used for employment purposes in order to continue providing an adequate protection of individuals and at the same time respect the employer´s right to manage and organise the work;

Justification:

[5] EM stands for Explanatory Memorandum and indicates that additional details on a specific point will be given in the explanatory memorandum to the Recommendation.

It is important that the preamble expresses both the need to protect the personal data of the employee and the right of the employer to manage and organise the work.

Recalling the 'Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance' adopted by the European Committee on Legal Co-operation (CDCJ) of the Council of Europe in May 2003, referred to in Resolution 1604 (2008) of the Parliamentary Assembly of the Council of Europe, which are fully topical and relevant and thus deeming it unnecessary to incorporate into a new recommendation further specific principles governing the use of video surveillance;

Recalling the European Social Charter of 18 October 1961, in particular its Articles 1.2 and 6, **and the International Labour Office's 1997 Code of Practice on the Protection of Workers' Personal Data;**

Recalling the European Convention on Human Rights, which protects in its Article 8 the right to private life, encompassing activities of a professional or business nature as interpreted by the relevant case law of the European Court of Human Rights;

Recommends that governments of member states:

- ensure that the principles contained in the **present** recommendation **and its Appendix, which replace the above-mentioned Recommendation Rec(89)2,** are reflected in the application of domestic legislation on data protection to the employment sector, as well as in other branches of the law bearing on the use of personal data for employment purposes;

- for this purpose, ensure that the **present** recommendation is brought to the attention of the authorities established under domestic data protection legislation which are competent to supervise implementation of such legislation;

- promote acceptance and implementation of the principles contained in the **appendix to this** recommendation **also** by **means of complementary instruments such as codes of conducts,** ensuring its wide circulation among representative bodies of both employers and employees**, as well as by involving designers and suppliers of technologies in the implementation processes of certain principles.**

APPENDIX TO THE RECOMMENDATION

1. *Scope and definitions*

1.1. The principles set out in this recommendation apply to **any collection and processing** of personal data for employment purposes in both the public and private sectors.

These principles apply to automatically processed data as well as to other data on employees which are held by employers, in so far as such information is necessary to make automatically processed data intelligible, **or used in any way to take decisions having a significant effect on the rights of the data subject concerned (EM: by analogy, they apply, where appropriate, to any personal data relating to individuals outside the workplace which are processed for work safety purposes, and also, to trade union organisations.)**

The manual processing of **personal** data should not be used by employers in order to avoid the principles contained in this recommendation.

1.2. Notwithstanding the principle laid down in paragraph 1.1, second sub-paragraph, a member state may extend the principles of this recommendation to manual processing in general.

1.3. For the purposes of this recommendation:

'Personal data' means any information relating to an identified or identifiable individual ("data subject"). An individual is not considered "identifiable" if identification requires unreasonable time or effort. [EM: by analogy : professional associations]

- 'Employment purposes' concerns the relations between employers and employees which relate to recruitment of employees, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work. **[EM: also relates to data processed after termination of the employment contract]**

1.4. Unless provisions of domestic law exist to the contrary, the principles of this recommendation apply, where appropriate, to the activities of employment agencies, whether in the public or private sector, which collect and **process, also through online information systems,** personal data so as to enable **one or more contracts of employment, including simultaneous or part-time contracts,** to be established between the persons registered with them and prospective employers**, or to help discharge the duties relating to those contracts. [EM: Information systems and technologies, genetic data, sensitive data]**

2. *Respect* for human rights, dignity and fundamental freedoms

Respect for human rights, dignity and fundamental freedoms, including the right to private life, the right to the protection of personal data, the right to non-discrimination should be safeguarded in the processing of personal data for employment purposes, [notably to allow to employees the free development of their personality and to foster possibilities of individual and social relationship on the workplace].

Question: We have some doubts as regards the text put in brackets. Has this wording been used in any other international legal instrument?

3. *Necessity, development of other principles and simplifications*

3.1. Information systems and technologies used for the collection and processing of personal data for employment purposes should be configured, and as the case may be certified, so as to minimise the use and storage of personal data, as well as to limit the use of directly identifying data to only that necessary for the aims pursued in the individual cases concerned. The same applies when they are used and implemented in the working environment. [EM: specify that tools and devices are covered by the notion of information systems and technologies – ref 3.3]

Question: What is the added value of the second sentence in relation to the first? This should be clarified in the Recommendation or the Explanatory Memorandum.

3.2. The employer should develop appropriate measures, including organisational ones, to ensure that they respect in practice the principles relating to data processing for employment purposes, and to enable this to be demonstrated adequately at the request of the supervisory authority.

3.3. Measures should be adopted according to the size of the concerned entity and the nature of the activities undertaken, taking also into account the possible consequences for data subjects.

4. *Information and consultation of employees*

4.1. **The introduction and use of information systems and technologies for the direct and principal purpose of remotely monitoring employees' activity, behaviour or localisation should not [in principle] be permitted when leading to a permanent monitoring of employees [except where no alternative means which are less intrusive are available and where appropriate safeguards exist].**
[EM: complementary to 4.1 – without prejudice of measures relating to well founded defence proceedings.[EM: The use of information systems and technologies, such as video surveillance on the workplace or geolocalisation systems, should be limited only to organisational and/or production necessities, or for security purposes on the workplace. Such systems should only be allowed if legitimate, necessary and regulated. They should not aim at permanently monitoring the quality and quantity of the individual work on the workplace, nor aim at remotely monitoring employees' behaviour or localisation.]

4.2. In case of the introduction, adaptation **and operation of information systems and technologies** for the collection and processing of **personal data necessary for requirements relating to production or safety or work organisation, employees or their representatives,** in accordance with domestic law or practice and, where appropriate, in accordance with the relevant collective agreements, should, in advance, be fully informed or consulted**. [EM: tools also covered by information systems and technologies]**

4.3. **The employer should take appropriate measures to assess the impact of any data processing which poses specific risks to the right to privacy, human dignity and protection of personal data, and to process such data in accordance with the principles laid down in this recommendation in the least invasive manner possible.**
The agreement of employees**' representatives** should be sought before the introduction or adaptation of such **information systems and technologies** where the **information or** consultation procedure referred to in **principle 4.2** reveals **such risks** unless domestic law or practice provides other appropriate safeguards.
[EM: for small enterprises, representatives refers to employees as such.]

5. *Collection of data and particular forms of processing or of information*

5.1. Personal data should in principle be **collected** from the **data subject concerned. When it is appropriate to process data external to the employment relationship or consult third parties, for example concerning professional references, the data subject** should be informed.

5.2. Personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of employment as well as the evolving information needs of the employer.

5.3. In the course of a recruitment **or promotion** procedure, the data collected should be limited to such as are necessary to evaluate the suitability of **the persons concerned** and their career potential.

In the course of **a recruitment**, personal data should, in principle, be obtained solely from the individual concerned. Subject to provisions of domestic law, **external** sources, **including those from consultancies or social networks for the development of professional relationships,** may be consulted with the consent o**f the individual concerned or if he or she** has been informed in advance of this possibility. **Profiling of the person concerned based on the secret collection of data from search engines should [in principle] be prohibited. An employer should not persuade the person concerned to provide or to enable access to any medical information held by third parties. [EM: added value of this Recommendation concerning electronic medical data / Ref recommendation (97)5 – explain profiling]**

In any event, appropriate measures should be taken so that also in the case of data readily accessible in electronic communications networks available to the public, only relevant, accurate and up-to-date data are used, thus also avoiding misinterpretation or unfair processing of that data viewed in the light of the context of its origin.
Question: The relation between article 5.1 and article 5.3 should be clarified, preferrably in the Recommendation or at least in the EM. Is article 5.1 the general rule whereas art 5.3 specifically regulates the situations of recruitment and promotion (if so, why is an example most relevant for recruitment and promotion used in article 5.1)? As regards 5.3 second paragraph there is also a need of clarification as to the meaning of "Subject to provisions of domestic law".

Moreover, it should be considered whether the current wording of article 5 may lead to unrealistic results. For example, does it prevent an employer from collecting information on a person it wishes to "headhunt" before approaching this person with an offer (the current wording requires consent or prior information)?

5.4. Recourse to tests, analyses and similar procedures designed to assess the character or personality of the individual should not take place without his or her consent or unless domestic law provides other appropriate safeguards. If **the individual** so wishes, he or she should be informed **in advance of the use that will be made** of the results of these tests**, analyses or similar procedures and, subsequently, the content thereof. [EM: no decision producing legal effects can be taken on the sole basis of such tests, analysis and similar procedures. The individual's profile should be based on objective data an in no circumstances reveal health related information. Such tests must be relevant and based on scientifically recognised methods. Regarding information on the content, possibility to delay in the provision of this information when protecting legitimate interests, including the ones of the employer]**

5.5 The processing of biometric data to identify or authenticate individuals should in principle only be permitted where it is necessary to protect the legitimate interests of the employer, employees or third parties and should be based on scientifically recognised methods which appropriately ensure security. [EM: definition of legitimate interests]
5.6. With regard to possible processing of personal data relating to Internet or Intranet pages viewed by the employee, preference should be given to the adoption of preventative measures, such as:

- **the configuration of systems or use of filters which prevent particular operations, as the case may be; [EM: such as uploading and downloading of particular content]**

- **the identification of sites which are or are not deemed to relate to the work carried out;**

- **the grading of possible monitoring on personal data, providing first for non-individual random checks on data which are anonymous or in some way aggregated. [EM: for example, by production unit].**

The persons concerned should be properly informed, in conformity with principles 4 and 12.

Where an employee uses, with the employer's authorisation, equipment which may reveal whereabouts, in particular outside working hours, appropriate arrangements should be made so that data relating to such whereabouts are not used and are automatically deleted as soon as possible. Appropriate internal procedures relating to the processing of that data should be established and notified to the persons concerned in advance. (EM: procedure which concerns policy in monitoring – procedure also valid for other types of processing?)

Justification: the current wording of the article seems to run a risk of being too strict since there may be several situations in which the employer, for safety reasons or for production necessities, have fully legitimate needs to use such data. There may also be cases where use of data should be permissible even if relating to whereabouts outside working hours, for example in cases of emergency. Maybe it instead could be considered to insert a weighing of the employer's need to process data on one hand and respect for the employee's privacy on the other hand?

Question: We would like a clarification as to the relationship between article 4.1 and 5.6. Article 4.1 seems to deal with the same question?

As regards the wording "automatically deleted as soon as possible" we would like to raise the question whether it is in practice possible to demand the deletion of information that may have been stored in and on several different kinds of technical equipment, for example mobile phones, computers, GPS-systems etc. And if so, is it possible to arrange for automatic deletion?

5.7 The employer should take the necessary measures and foresee the appropriate procedures aimed at enabling, in case of absence of the employee, access to professional emails when such access is of absolute professional necessity, and after having informed the employee of such procedures. Access to personal emails of the employee shall never be permitted.

Justification: There should not be an obligation to give information in each individual case before accessing the information. Where there is an absolute professional necessity, the matter is often urgent. In such cases it may not be possible to give information to the employee. Further, the employee may also be difficult to reach during his or her absence. Information should instead be given in relation to the procedures regarding access, and in particular under which circumstances access may be legitimate.

[EM: structure : surveillance of employees ?
Where possible, and appropriate, it should be considered whether preference should be given to assigning employees email addresses which are directly traceable to posts rather than to individuals. Appropriate instructions should be issued so that where an employee is absent the email system automatically communicates the details of another point of contact, indicating that the employee is temporarily absent.
In order to inform the addressee that the email account is used purely for professional purposes, an appropriate warning should be inserted in emails sent by the employee.]

Justification: It is very common that e-mail adresses include the names of individuals. To change the

e-mail addresses might cause inconveniences for the employers'. In some cases there might even be an advantage to use a persons name in the e-mail address since it enables the sender to easily communicate (easy to remember the e-mail adress) and to know to whom they are communicating.

6. ***Storage of data***

6.1. The storage of personal data is permissible only if the data have been collected in accordance with the rules outlined in **principles 4.1 and 5** and if the storage is intended to serve employment purposes. [**Where this is not the case, the employer should refrain from using the stored data.]**

Justification: The second sentence of article 6.1 seems to justify the storage of data which has not been collected in accordance with the Recommendation. It should be considered to reword this part of the article. Or is it meant to be a "safety device" in case data has accidently been stored in contradiction to the rules outlined in the principles?

6.2. The data stored should be accurate, where necessary kept up to date, and represent faithfully the situation of the employee. They should not be stored or coded in a way that would infringe an employee's rights by allowing him or her to be characterised or profiled without his or her knowledge.

Where the use of biometric data is permitted under paragraph 5.5, they should not, as a rule, be stored in a database, and preference should be given, where appropriate, to biometric identification or authentication systems based on media made available solely to the person concerned. [EM: specify when such a storage is permissible].

6.3. Where judgmental data are stored relating to the performance or potential of individual employees, such data should be based on fair and honest evaluations. **[EM: and must not be insulting in the way they are formulated]**

7. ***Internal use of data***

7.1. Personal data collected for employment purposes should only be **processed** by employers for such purposes.

With due regard to the principles of relevance and accuracy. and with regard in particular to large-scale or territorially extensive working environments, certain personal data could be made easily accessible in internal communication networks in order to speed up the performance of the work carried out and facilitate interaction with other employees. [EM: identification data – large scale context : intranet tools for instance : tel/email/picture only with consent].

7.2. Where data are to be **processed** for employment purposes other than the one for which they were originally collected, adequate measures should be taken to avoid misinterpretation of the data in the different context and to ensure that they are not used in a manner incompatible with the original purpose. Where important decisions affecting the employee are to be taken, based on data so **processed**, he or she should be informed. **[EM: illustrate with concrete examples]**

7.3. The interconnection of files containing personal data collected and stored for employment purposes is subject to the provisions of **principle 7.**2.

7.4. Without prejudice to principle 9, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principle of purpose specification in the subsequent use of the data. Where substantive changes in the processing occur, the persons concerned should be informed. [EM: in the due respect of applicable law and as may be found appropriate by data protection authorities]

8. ***Communication of data and use of information systems for the purpose of employee representation***

8.1. In accordance with domestic law and practice or the terms of collective agreements, personal data may be communicated to employees' representatives in so far as such data are necessary to allow them to represent the interests of the employees.

8.2. The use of information systems and technologies for trade union communications should be safe-guarded by transparent rules permitting correct use to protect any confidential communications. [EM: the type of agreement is not to be determined by the data protection authorities]

Justification: Recognising the social partner's right to freely negotiate it does not seem appropriate to demand the partner's to reach a collective agreement. A more suitable solution would be to recommend that information systems and technologies for trade union communications should be safe-guarded by transparent rules permitting correct use to protect any confidential information.

9. *External communication* and dissemination *of data*

9.1. Personal data collected for employment purposes should be communicated to public bodies for the purposes of their official functions only within the limits of employers' legal obligations or in accordance with other provisions of domestic law.

9.2. The communication of personal data to public bodies for purposes other than the exercise of their official functions or to parties other than public bodies, including enterprises in the same group, should only take place:

a. where the communication is necessary for employment purposes which are not incompatible with the purposes for which the data were originally collected and where employees or their representatives are informed of this; or

b. with the express consent of the individual employee; or
c. if the communication is authorised by domestic law,

[EM: give other examples]

Justification: If something is authorised by domestic law, it seems superfluous to give examples of certain cases, there may be other situations.

9.3. **On the basis of adequate safeguards provided by domestic law, personal data can be communicated within a group of enterprises for the purpose of discharging duties provided for by law. The consent of the employee may also be required as safeguard.**

[EM: it cannot be excluded that in precise areas, a freely given consent may play a role. Illustrate with examples of situations such as sharing CVs. Duties relating to social security and welfare for employees, or to optimise the allocation of human resources.]

Justification: see the general remark in the preamble as to how the notion of "law" is to be interpreted in Sweden in the field of labour law. Instead of consequently repeating all the different sources throughout the Recommendation a more suitable solution maybe could be to consequently keep to the notion of "law"?

9.4. **With regard in particular to the public sector, the law should reconcile the right to privacy and protection of personal data with the requirements relating to transparency or monitoring of the correct use of public resources and funds, for example by identifying professional categories or profiles in respect of which there are requirements relating to the publication of certain information, and also the type of the relevant notices which, for homogeneous classes, can be made public, that is to say by also considering the possibility of identifying them more easily where they can be traced through external search engines.**

Justification: There are many other ways to reconcile these interests.

9.5. **When the work tasks entail a constant relationship with the public or where this is necessary to meet the requirements relating to transparency vis-à-vis users, consumers and citizens, appropriate measures and safeguards may be adopted to make the employee concerned directly or indirectly identifiable. [EM: To that end, one may also relate – if appropriate - on an identification code allocated to and displayed by the employee or another personal reference.]**

10. *Particular categories of data*

10.1. Personal data relating to racial origin, political opinions, religious or other beliefs, sexual life or criminal convictions, referred to in Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, should only be collected and **processed** in particular cases, **where it is indispensable for the recruitment or to fulfil legal obligations related to the contract of employment,** within the limits laid down by domestic law and in accordance with appropriate safeguards provided therein. In the absence of such safeguards, such data should only be collected and **processed** with the express consent of the employees **and provided it is in the employee's interest**.
[EM : also covers pension systems / sickness insurance schemes negotiated by employers/ trade unions]
10.2. An employee or job applicant may only be asked questions concerning his or her state of health and be medically examined in order:

a. to determine the**ir** suitability for the present or future employment;

b. to fulfil the requirements of preventive medicine;

e. to allow social benefits to be granted**; or [EM: explain social benefits]**

f. **to satisfy judicial procedures.**

In principle, it should be prohibited to collect and process genetic data, in particular to determine the professional suitability of employees or job applicants, even with the consent of the person concerned. Provision may be made for exceptions only within the limits laid down by domestic law and where there are appropriate safeguards, which should also provide for the prior involvement of the supervisory authorities, for the sole purpose of adopting, at the request of the employee, the measures necessary with regard to his or her health, safety or working conditions.
[EM: according to Recommendation(97)5, such processing can only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties]

10.3. Health data **and - where their processing is lawful - genetic data,** may not be collected from sources other than the employee concerned except with his or her express consent or in accordance with provisions of domestic law.

10.4. Health data covered by medical secrecy **and - where their processing is lawful - genetic data,** should only be **processed** by personnel who are bound by medical secrecy or by others who, in accordance with domestic law, may have access to such data.
The information should only be communicated to other categories of personnel if it is indispensable for decision-making by the latter and in accordance with provisions of domestic law.

Justification: there are in Swedish legislation situations under which health data may be communicated and processed by other categories than personnel covered by medical secrecy.

10.5. Health data covered by medical secrecy **and - where their processing is lawful - genetic data,** should be stored separately from other categories of personal data held by the employer. Security measures should be taken to prevent persons outside the medical service having access to the data.

10.6. The data subject's right of access to his or her health data **and genetic data** should not be restricted unless access to such data could cause serious harm to the data subject, in which case the data may be communicated through a **medical practitioner** of his or her choice.

10.7. The employer should process any health data relating to third parties in so far as is necessary to discharge obligations laid down by law, while maintaining the safeguards relating to the health data of employees. [EM : examples of processing health data relating to third parties such as family members of the employee in order to attribute specific benefits to them].
Justification: see the general remark in the preamble as to how the notion of “law” is to be interpreted in Sweden in the field of labour law. Instead of consequently repeating all the different sources throughout the Recommendation a more suitable solution maybe could be to consequently keep to the notion of “law”?

11. ***Transparency of processing***

11.1. Information concerning personal data held by the employer should be made available either to the employee concerned directly or through the intermediary of his or her representatives, or brought to his or her notice through other appropriate means.

This information should specify the main purposes of **the processing of** data, the sort of data **processed**, the categories of persons or bodies to whom the data are regularly communicated and the purposes and legal basis of such communication.

[EM: In this context, a particularly clear and complete description must be provided of the type of personal data which can be collected by means of information systems and technologies which enable them to be monitored indirectly by the employer, and of their possible use. A similar description should be provided of the use of biometric and of Radio Frequency Identification (RFID) technology, the possible use of personal identification codes, and also the role of any system administrators in relation to data processing.]

Justification: Due to its quite high degree of details as to the technologies used we would like to propose that the last paragraph is moved to the Explanatory Memorandum.

11.2. The information should also refer to the rights of the employee in regard to his or her data, as provided for in **principle 12** of this recommendation, as well as the ways and means of exercising his or her right**s**.

11.3 The information referred to in the preceding paragraph should be provided and updated in due time and, in any event, before the employee carries out the activity or action concerned, and made readily available also through the information systems normally used by the employee.
[EM: illustrate possible "activity or action concerned"]

12. *Right of access and rectification*

12.1. Each employee should, on request, be enabled to have access to all personal data held by the employer which concern him or her and, as the case may be, to have such data rectified or erased where they are held contrary to the principles set out in this recommendation, **in particular where it is incorrect**. **Each employee should also be granted the right to know any available information as to their source, the parties to which the data have been, or could be, communicated and/or as to the knowledge of the logic involved in any automated process concerning him or her.**
To that end, in particular in large-scale or territorially extensive places of work, the employer should introduce general preventative procedures to ensure that there is an adequate and prompt response where the rights are exercised. [EM: general policy will explain how covered processing – surveillance could happen.]

12.2 The right of access should also be guaranteed in respect of evaluation data, including where they relate to assessments of the productivity or capability of the employee provided for in principle 5.3, at least when the assessment process has been completed, without prejudice to the right of defence of employers or third parties involved; although they cannot be directly rectified by the employee, purely subjective assessments should be open to challenge in the manner laid down in domestic law. [EM: postponement for defence purpose on temporary basis.]

12.3. Exercise of the rights referred to in paragraph **12.1** may, in the case of an internal investigation conducted by the employer, be deferred until the close of the investigation if the result of the investigation would be otherwise threatened. **However, internal investigations should not be carried out on the basis of an anonymous report, except where it is circumstantiated and relates to serious infringements which should be identified by domestic law or a decision of the supervisory authority. [EM: communication of the results of the internal investigation to a third party – reference to principle 9.2's requirements to develop the notions of "circumstantiated / serious infringements" and refer to WP 29's opinion 1/2006 on the application of EU data protection rules to internal whistle blowing schemes in the fields of**

accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime].

12.4. When an employee is faced with a decision based on automatic processing of data held by an employer, he should have the right to satisfy himself that the data have been lawfully processed.

12.5. Except where provisions of domestic law exist to the contrary, an employee should be entitled to **choose and** designate a person to assist in the exercise of the right of access or to exercise the right on his or her behalf.

12.6. If access to data is refused or if a request for rectification or erasure of any of the data is denied, domestic law should provide a remedy.

13. *Security of data*

13.1. Employers or firms which may process data on their behalf should implement adequate technical and organisational measures**, which are updated as new technologies are developed,** designed to ensure the security and confidentiality of personal data stored for employment purposes against unauthorised access, use, communication or alteration. **[EM: employers should be given time to adapt to new technologies / connected to principle 2.3. and possible reference to Article 17.3 Directive 95/46 EC on 'processor']**

13.2. The personnel administration, as well as any other person engaged in processing the data, should be kept informed of such measures and of the need to respect them.

14. *Conservation of data*

14.1. Personal data should not be stored by an employer for a period longer than is justified by the purposes outlined in paragraph 1.3 or is required in the interests of a present or former employee.

14.2. Personal data submitted in furtherance of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made.

14.3. Where such data are stored with a view to a further job application, **the person concerned should be informed in due time and** the data should be deleted if the candidate concerned so requests.

Where it is necessary to store data submitted in furtherance of a job application for the purpose of defending legal actions, the data should only be stored for a reasonable period.

14.4 Personal data processed for the purpose of an internal investigation carried out by the employer which has not led to the adoption of negative measures in relation to any employee should in principle be deleted in due time, without prejudice to the right of access up to the time at which they are deleted.

SWITZERLAND / SUISSE

Nous avons examiné le projet de recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi dans sa version du 30 juin 2011. A cet effet, nous avons procédé à une consultation des organes intéressés en Suisse.

1. Remarques générales

Dans l'ensemble nous saluons le projet de recommandation. Il conviendra cependant d'examiner l'opportunité de réécrire l'ensemble de la recommandation, notamment pour la mettre en concordance avec les recommandations les plus récentes.

La structure de la recommandation ne nous paraît pas suffisamment claire. Un degré de concrétisation trop élevé ne permet pas de tenir compte des évolutions techniques à venir. Par ailleurs, Nous avons constaté plusieurs erreurs de traduction entre la version française et la version anglaise, une relecture attentive s'avère indispensable.

2. Propositions de modifications :

Préambule	**Observations et propositions**
Cons. 3	Biffer « notamment automatisé »
Cons. 9	Biffer ; relève plutôt de l'exposé de motifs.
Annexe à la recommandation	**Observations et propositions**
1.	Nous sommes d'avis que le champ d'application devrait être limité au rapport de travail stricto sensu, prévoyant comme acteurs l'employeur, l'employé ainsi que les apprentis, mais pas des tiers comme les organisation syndicales ou des personnes intéressées du point de vue de la sécurité. Tout au plus peut-on concevoir un tel assujettissement en ce qui concerne les règles sur la sécurité des données.
1.2.	Du point de vue de la technique législative, on peut se demander s'il ne serait pas préférable d'élargir le champ d'application aussi aux traitements non automatisés de données selon le principe 1.2.
1.3.	Il conviendrait de s'interroger sur la nécessité de définir le terme « employé ». Nous proposons également d'introduire une définition des données sensibles : « L'expression « données sensibles » désigne les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou les autres convictions, et les données à caractère personnel relatives à la santé ou à la vie sexuelle ou concernant des condamnations pénales, ainsi que les autres données définies comme sensibles par le droit interne. Les données de santé se réfèrent également aux données génétiques. Les données biométriques sont assimilées à des données sensibles. »

	Qu'en est-il du « body-leasing »? Les personnes qui sont engagées de manière indirecte doivent aussi bénéficier de la même protection. Il conviendra de préciser au moins dans l'exposé des motifs.
1.4.	Il conviendrait de définir le terme « contrat simultané ». Etendre le champ des destinataires de la sorte risque de créer, au pire des cas, des insécurités juridiques. L'élaboration de dispositions propres dans le domaine des agences d'emploi devrait être envisagée.
3.1	Cet article ne devrait pas mener à une obligation de l'employeur (ou respectivement un droit de l'employé), de devoir utiliser ou ne pas utiliser certains programmes informatique ou dispositifs électroniques. Au contraire, l'employeur devrait pouvoir choisir librement les programmes informatiques et les dispositifs électroniques qu'il considère adéquats mais il doit les utiliser et les configurer et/ou organiser ces opérations de manière à respecter les règles de protection des données et notamment le principe de minimisation des données. Nous proposons de substituer le terme de « atteindre les objectifs propres à chaque situation » par « atteindre les objectifs propres à chaque rapport de travail ».
3.2	Dans l'exposé des motifs, il conviendrait de définir ce que l'ont entend par « prouver de manière adéquate" de manière à ce que cela soit également possible pour des PME». La rédaction de ce paragraphe n'est pas suffisamment précise et comporte, de ce fait un risque de devenir, dans son application concrète, trop contraignant pour les employeurs.
4.	Nous souhaiterions vous rendre attentif au fait que le droit suisse (art. 26 de l'ordonnance 3 relative à la loi sur le travail, RS 822.113) interdit l'utilisation des systèmes de surveillance ou de contrôle destinés à surveiller le comportements travailleurs à leur poste de travail. Lorsque ces systèmes sont nécessaires pour d'autres raisons, ces derniers doivent notamment être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs. Nous sommes d'avis que les conditions d'adéquation au but, de subsidiarité et de proportionnalité devraient ressortir de manière plus clair de ce principe.
4.1	L'article 4.1 n'est pas à sa place car il ne concerne pas «l'information et la consultation des employé» ; il serait plus judicieux de le placer à l'article 5 ou dans un nouvel article spécifique concernant la surveillance. L'objet de cette réglementation mériterait une réglementation plus articulée, respectivement différenciée. On ne distingue par exemple pas entre surveillance de la prestation de travail (ou de l'avancement des travaux) et surveillance du comportement. Cette dernière obéit à des règles autres que pour la surveillance de la prestation ou de la sécurité. Comme elle est formulée, la norme pourrait créer des insécurités juridiques. Doit-on par exemple conclure que la surveillance non permanent du comportement est licite sans autre condition?

	A noter que le Tribunal fédéral suisse a déjà eu l'occasion de préciser qu'un système de géolocalisation est licite si le contrôle s'exerce de manière non permanente et uniquement sur les déplacements professionnels. Pour le Tribunal fédéral, un tel système de géolocalisation ne diffère guère d'une machine à timbrer et poursuit en principe un but de sécurité des personnes et des biens (ATF 130 II 425). Nous préconisons la suppression de la dernière phrase entre crochet. Il n'est pas admissible, sous prétexte qu'il n'y aurait pas d'alternatives, que l'introduction de systèmes d'information conduise essentiellement à contrôler à distance le travail.
4.3	La première phrase de ce principe pourrait être déplacé dans le principe 2.
5.1	Les conditions mises à la prise de référence mériteraient d'être précisées. En particulier, il faut tenir compte du fait que l'employeur potentiel ne peut prendre des renseignements auprès de l'employeur actuel ou précédent qu'après avoir obtenu l'accord du candidat (un accord tacite étant admissible si le candidat indique des références dans son dossier de candidature).
5.3	Est-ce qu'on peut exclure d'utiliser des données existantes en cas d'avancement. En effet, l'employeur devrait aussi pouvoir utiliser les données existantes dans le dossier de l'employé, notamment qualification, formation, etc., pour autant que cela se fasse de manière transparente. A la lecture de ce principe, il n'apparaît pas clairement si, lors du recrutement, la collecte de données sur internet sans le consentement de la personne est autorisée. Une déclaration claire à cet égard s'impose. Dans la pratique, il est très courant de consulter les moteurs de recherche et, au lieu d'interdire cette pratique il faudrait inciter à une certaine transparence. L'employeur devrait donc informer le candidat qu'il a consulté les moteurs de recherche.
5.4	Qu'entend-t-on par méthodes scientifiquement reconnues dans la pratique ? Il conviendrait de préciser cette notion dans l'exposé des motifs. L'objet de ce principe confirme notre proposition d'élargir le champ d'application de la directive aussi aux données personnelles traitées de façon non automatisée.
5.5	Il conviendra de préciser dans l'exposé de motifs en quoi la biométrie est susceptible de protéger l'intégrité personnelle et la santé des employés ou de tiers. En outre, le recours à la biométrie devrait prendre en compte les principes figurant en conclusion du rapport d'étape sur la biométrie. Il faut ajouter le concept fondamental de traitement décentralisé des données biométrique (c'est-à-dire qui ne sont pas stockées dans un serveur central de l'employeur, mais traitées exclusivement au niveau du lecteur des empreintes digitales ou autres données biométriques). Il convient aussi de veiller à ce que la formulation puisse englober des nouvelles évolutions ainsi que de renvoyer au principe de la proportionnalité.

	Il faut corriger un problème de mise en page entre ce principe et le suivant.
5.6 – 5.7	Cette disposition contient plusieurs idées et il conviendra d'en revoir l'articulation. Certains éléments touchent par exemple plutôt à la sécurité des données, notamment en relation avec l'utilisation d'Internet / Intranet. C'est le cas de la configuration des systèmes et de l'identification de catégories de sites. D'autres relèvent de la surveillance des employés, à l'instar du principe 4.2 ou de règles de comportement de l'employé. ll convient d'ajouter que l'analyse nominative des données, après découverte de façon non nominative (anonyme ou pseudonyme) d'un abus ou après naissance d'un soupçon concret d'abus (toujours sur la base d'analyses non nominatives), doit servir exclusivement à l'identification de l'employé responsable. En d'autres termes, il faut éviter le caractère durable de l'analyse nominative. De plus, cela n'est techniquement notamment pas possible avec un Iphone. De plus, la question de l'effacement n'est souvent pas dans la compétence de l'employeur, ex. puce anti-vol dans les voitures.
6.1	Il faudrait y inclure les principes 2 et 3.
6.2	Concernant les données biométriques, il faudrait, dans l'exposé des motifs au moins, expliciter quant un enregistrement est envisageable dans une base de données. Par exemple est-ce envisageable pour des raisons de preuve ? ou pour permettre la réutilisation des données biométriques à des fins opérationnelles, notamment pour améliorer l'efficacité ou la qualité ?
6.3	La gestion des données appréciatives relatives à la productivité ou à la potentialité des employés mériterait un développement plus détaillé s'agissant des conditions de traitement. Il faudrait revoir la terminologie utilisée dans l'exposé des motifs.
7.1	Le 2^{e} alinéa, même s'il est pertinent, relève plutôt de l'exposé des motifs. Il faut préciser que seules les personnes autorisées de par leur fonction doivent pouvoir accéder aux données sur le réseau interne.
7.2	Il faut préciser les mesures dont on parle.
7.4	Il nous semble important de préciser dans l'exposé des motifs que, si pour des raisons particulières, on ne peut pas informer les personnes concernées et recueillir leur consentement, la communication n'est possible que sous forme anonyme. Un exemple de mauvaise traduction: The person**s** concerned **should** be.. - La personn**e** concernée **doit** être…
8.1	Nous sommes d'avis qu'un tel accès ne devrait être autorisé qu'en cas de consentement de l'employé ou lorsque les données sont mises à dispositions sous forme anonyme.
8.2	Cette question devrait être réglé au cas par cas par les syndicats ou l'employeur. Les activités syndicales, respectivement l'appartenance à un syndicat, sont des données sensibles qui ne doivent, en principe, pas être traitées par l'employeur. Ce principe pourrait apparaître explicitement ici.
9.	Nous proposons l'intitulé suivant : « communication des données à

	caractère personnel »
9.3	Indiquer simplement que le consentement peut être requis est insuffisant. Il convient de préciser qu'il doit être requis dans certains cas, en énumérant ces cas de manière au moins exemplative.
9.4	Dans l'exposé de motifs, on pourrait reprendre – sous l'angle des garanties appropriées -, l'idée de concilier les intérêts en présence notamment en distinguant des catégories ou des profils professionnels pour lesquels il est nécessaire de publier certaines informations, ainsi que la typologie des informations pertinentes qui peuvent être rendues publiques, en fonction des classes homogènes et ce, en tenant compte de la possibilité d'en prendre connaissance plus facilement s'il est possible de les retrouver à l'aide de moteurs de recherche externes.
9.5	Il faut distinguer les professions qui présentent des dangers pour la sécurité personnelles des employés (pour lesquelles un code d'identification est suffisant) de celles qui sont sans danger.
10.1	Si on introduit – comme proposé ci-dessus – une définition des données sensibles, le principe devrait être reformulé comme suit : 11. Données sensibles 11.1 « Les données sensibles ne devraient être collectées … » Nous proposons également de couvrir la phrase précontractuelle (recrutement) lorsque de telles données sont pertinentes pour déterminer l'aptitude du candidat à un emploi. On peut se demander s'il ne serait pas préférable d'élargir le champ d'application aux traitements non automatisés de données.
10.5	Nous proposons la formulation suivante « Les données de santé couvertes par le secret médical et les données génétiques, lorsque leur traitement **est nécessaire** et autorisé par le droit interne, devraient être enregistrées … »
11.	Ce chapitre doit être revu pour tenir compte des exigences actuelles en matière d'information (voir notamment les dernières recommandations).
11.1	« indirectement les employés**,**. » Supprimer la virgule.
12.1	Deuxième paragraphe remplacer Á par **À**.
12.2	La phrase « s'agissant de données **à d**'appréciation» n'est pas formulée correctement.
12.3	Le droit suisse n'interdit pas en principe les enquêtes internes ouvertes à la suite d'un signalement anonyme. L'employeur doit toutefois respecter le principe d'exactitude fixé à l'article 5 LPD et fournir des informations sur l'origine des données si la personne concernée exerce son droit d'accès.
13.1	Dans l'exposé des motifs, il faudrait préciser que les entreprises devraient néanmoins être autorisées à utiliser leur infrastructure pour une période de temps raisonnable, si l'investissement respectif n'était pas déraisonnable au moment de leur acquisition/développement. Phrase entre parenthèse : « en lien avec le principe **3.2** et non pas 2.3 ».

THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA / L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE

Regarding the Draft Recommendation on the protection of Personal data used for employment purposes, the Directorate for Personal Data Protection of the Republic of Macedonia would lie to note with satisfaction that Draft Recommandation on the protection of personal data used for employment purposes is prepared in accordance with the increasing use of new technologies and means of electronic communication in relations between employers and employees, and corresponding advantages thereof. The Draft Recommendation is certainly positive step and includes useful novel provisions in the field of data processing methods, particularly automatic processing of personal data protection.

We have only one comment and suggestion in order the text of the Draft Recommendation to be improved in the following manner:

In the part 5.5 of *Collection of data and particular forms of processing or of information* , in the end of the sentence after words „ensure security" we suggest to be put the following words „and in accordance with the provisions of domestic law".

UNITED-KINGDOM / ROYAUME UNI

Comments on the draft Recommendation

There are a several typographical errors, which we have corrected in tracked changes on the annexed Recommendation.

Section 5.1 – There may be consultation with third parties where it would be inappropriate to inform the employee, for example the detection or investigation of criminal activity. This point is also relevant to **section 6.2** regarding storage of data. There may be situations where an employer is asked by law enforcement authorities to store information on an employee and this would not be covered by the current wording of 6.2 which says that data should only be stored if it is intended to serve employment purposes.

Section 5.4 – There may be situations where the individual may not give their consent to the processing of his or her personal data, but where there is a legitimate interest for the employer to

ensure that they have the best candidate for the position through a fair and transparent recruitment process. Such processing may also act as a safeguard for the employee, for example, the videotaping of recruitment assessments to allow for the process to be independently reviewed and ensure a consistent approach was taken by the examiners to all candidates. Individuals should be made aware in advance of any such processing and its purpose.

Section 5.6 – We consider that the word "automatically" should be removed from this paragraph as the deletion of some of this data may need to be done manually.

Section 5.7 – There may be situations in which it is justifiable for an employer to read the personal emails of an employee, for example if there is reasonable suspicion that the employee is acting illegally or outside the policies set by the organisation. The bureau could consider wording such as "access to personal emails of the employee shall *only be justifiable where the employer has reasonable grounds to suspect an employee's activity to be contrary to its internal policies or is otherwise involves unlawful practice*."

This section could recognise the fact that there may still be some businesses that operate without email access.

We are not convinced of the practicality of assigning email addresses which are traceable by post, rather than name. The proliferation of common job titles in larger organisations may lead to emails going astray and personal information being misplaced/misused. There is also a question around transparency for customers about who they are dealing with. The Bureau may also wish to consider the cost implications of changing to such a system.

Section 6.2 – An illustrative example of the type of biometric identification or authentication system envisaged in this paragraph would be helpful. This may be something that could be added to the EM.

Section 7.1 – The note on the EM at the end of this paragraph seems to imply that employers should not publish an employee's work email address or telephone number on internal systems without their consent, which may impede the day-to-day functioning of the organisation. We would like to see some clarification of what is meant by this note.

Section 9.2.c – The bureau may wish to consider adding "for the prevention or detection of crime" to the list of situations in which such a transfer may be authorised by public law.

Section 10.1.d – We consider that this point should cover "law enforcement" procedures, rather than "judicial" procedures.

Section 10.2 and 10.3 – 10.3 states that genetic data, where their processing is lawful, may be collected from third parties with the express consent of the individual, but the collection of genetic data directly from the individual, even with their consent, is prohibited in 10.2. This does not seem logical and may require some revision.

Section 12.1 – We consider that there may need to be some exemptions put in place for particular circumstances where it may not be appropriate to inform the employee that their information is being processed. For example, article 29(1) of the Data Protection Act in the UK provides an exemption in this respect for personal data processed for the prevention or detection of crime, the

apprehension or prosecution of offenders and the assessment or collection of any tax or duty or of any imposition of a similar nature etc.

Section 14.2 – The bureau may wish to consider that such data should be deleted as soon as "it is no longer required" rather than "as soon as it becomes clear that an offer of employment won't be made". There are many situations where, after taking the decision not to make a job offer, the employer may need to write to the applicant to inform them of their decision or to offer to keep their CV on file until a suitable appointment arises.

The UK notes that there is no reference in the report to data collected for ethnic monitoring/ equality and diversity purposes, or criminal records check as part of vetting procedures. We should be grateful to know whether the Bureau will be considering these areas in their Recommendation.

Ministry of Justice
27 September 2011

COUNCIL OF EUROPE COMMITTEES

SOCIAL CHARTER / CHARTE SOCIALE

This revision of the original Recommendation is necessary and timely.The European Committee of Social Rights has discussed this draft informally, it found it very interesting not least as it indicates the preoccupations of states and other bodies in order to ensure privacy at work, a right guaranteed by the European Social Charter. The European Committee of Social Rights has no specific comments on the substance, however it requests that the reference to the 1961 Charter be replaced by the European Social charter opened for signature in 1961 (ETS 35) and revised in 1996 (ETS 163) and that it be treated in a separate paragraph from the ILO Code.

EUROPEAN COMMITTEE ON LEGAL CO-OPERATION / COMITE EUROPÉEN DE COOPERATION JURIDIQUE - CDCJ

LATVIA / LETTONIE

Latvian delegation supports further progress of the revised Recommendation No. R (89) 2 on the protection of personal data used for employment purposes without any objections at this stage.

SLOVENIA / SLOVENIE

Preamble

General instruction should be added that not only essence of rights but as much as possible of determinations of different issues should be regulated by national laws and only within this framework agreements between employers and employees could be formed.

2.
We propose slightly changed text:

Respect for human dignity and the right to private life, the right to the protection of personal data, the right to non-discrimination and other relevant human rights and fundamental freedoms should be safeguarded in the processing of personal data for employment purposes, notably to allow to employees the free development of their personality and to foster possibilities of individual and social relationship on the workplace.

Explanation:
It is our believe that on the basis of recent development of privacy in workplace it is necessary to underline starting point – human dignity and the right of the protection of private life, followed by other human rights and fundamental freedoms. With this change impact of recommendation would be strengthened.

5.5.
Expression »to protect the legitimate interests of the employer« seems to be too extensive and therefore problem to be acceptable. To avoid misunderstandings and different explanations it would be useful to add

description of »legitimate interests« which would contain limitation from 4.1 ("it should be prohibited when it might lead to a permanent monitoring of employees".

5.6.
Starting point should be that due to the operation procedure and security policy there are some limitations needed. And this is basis for regulation on this field.

8.2.
Trade union communications should be at least in general lines protected by law and not only by agreements.

GERMANY / ALLEMAGNE

1. Généralités

L'Allemagne se félicite de la révision de la Recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi s'étant avérée nécessaire eu égard aux multiples développements techniques et aux exigences propres au secteur de l'emploi. Une version actualisée de la Recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi sera d'une grande utilité pratique car jusqu'à présent peu d'États membres seulement ont adopté en Europe des dispositions légales en la matière. Les propositions faites par l'expert Giovanni Buttarelli (Italie) constituent une très bonne base pour ce travail. Compte tenu de la grande complexité de la matière, la révision requiert des connaissances spécifiques et des expériences concrètes dans le domaine de la protection des données à caractère personnel utilisées à des fins d'emploi. C'est pourquoi il importe notamment de faire participer le plus tôt possible le Comité européen de coopération juridique du Conseil de l'Europe (CDCJ) et, par son intermédiaire, les États membres du Conseil de l'Europe pour obtenir sur cette base à un instrument utile à tous les États membres.

Un examen du projet paraît nécessaire car le texte prévoit presque systématiquement et indépendamment de la nature des données concernées la possibilité de traiter des données avec le consentement de l'intéressé. Dans ce contexte, il y aurait lieu de tenir compte du fait qu'il existe souvent une situation hétérogène dans le secteur de l'emploi de sorte que les employés ne donnent pas toujours volontairement leur consentement. Ceci revêt une importance particulière lorsqu'il s'agit de la collecte, le traitement ou l'utilisation de données sensibles des employés.

L'Allemagne est consciente des difficultés soulevées par la révision et donc prête à y collaborer de façon intense.

2. Les différentes dispositions du projet

Paragraphe 3.1, 1ère phrase :
Il convient de saluer l'introduction d'une approche « Privacy by design » au paragraphe 3.1. Il existe des tendances comparables au niveau de l'UE. En élaborant sa recommandation le Bureau du T-PD s'est inspiré, entre autres, de l'article 3 a de la loi fédérale sur la protection des données (*Bundesdatenschutzgesetz - BDSG*).

Le titre 4.
Le titre du paragraphe 4 et les règles contenus aux paragraphes 4.1 – 4.3. ne s'accordent pas. Les paragraphes 4.1 et 4.2. ne traitent notamment pas de l'« Information et consultation des employés » mais de mesures d'observation, de surveillance respectivement de contrôle des employés. Cet aspect devrait s'exprimer dans le titre.

Paragraphe 4.1.

Revêtent une importance centrale des dispositions régissant les conditions dans lesquelles une « surveillance » des employés est autorisée ou non. Les règles prévues au paragraphe 4.1. semblent cependant trop générales et excluent par principe seulement une surveillance « permanente » des employés par un « contrôle à distance ». Il serait souhaitable de prévoir des règles bien plus différenciées. Il convient alors de préciser qu'un contrôle du comportement et du travail des employés ne devraient être autorisés que si la collecte et l'utilisation des données sont nécessaires à des fins d'emploi, par exemple pour l'exercice des droits de l'employeur. Il faut en outre faire ressortir que des droits de participation éventuels des représentations des employés doivent être respectés. Il est suggéré d'insérer dans la Recommandation même des aspects prévus en l'état actuel pour l'« exposé des motifs » de la Recommandation, tels que par exemple les observations quant aux « exigences organisationnelles et/ou de production » et aux « fins de sécurité » à la page 5.

Il est encore suggéré d'expliquer certaines expressions dans l'exposé des motifs et de les assortir d'exemples, par exemple le terme « contrôle à distance » et le terme (surveillance) « permanente ». Ceci est indispensable du point de vue allemand. Une "surveillance permanente" des employés (par exemple une vidéosurveillance) est extrêmement problématique car, eu égard à la protection du droit général de la personnalité, elle pèse particulièrement sur les employés. Au vu de ces considérations, des contrôles au hasard seront préférables compte tenu de la protection des données. Il faudra en outre respecter également des droits de participation éventuels des représentations des employés. Dans ce contexte, il conviendrait cependant d'opérer une distinction entre la surveillance ostensible et une surveillance clandestine. Il y aurait lieu de préciser les conditions régissant un contrôle ostensible ou clandestin (des contrôles clandestins seulement à titre exceptionnel pour le dépistage d'infractions pénales).

Paragraphes 4.2 et 4.3
Les thèmes principaux des paragraphes 4.2 et 4.3 ne sont pas le contrôle/la surveillance des employés mais les obligations de l'employeur d'informer/de consulter (4.2), d'une part, et les évaluations de l'impact (4.3), d'autre part. Il est suggéré soit de faire clairement ressortir ces aspects dans de (nouveaux) titres soit de placer ces dispositions à un autre endroit plus approprié dans le texte.

Paragraphe 5.3.
5.3. Il y a lieu d'observer que selon les expériences faites par l'Allemagne il peut être difficile d'opérer une distinction entre des réseaux sociaux privés et professionnels (en tant que source d'information pour l'employeur).

Paragraphe 5.5
Le paragraphe 5.5 ne paraît pas assez circonstancié. Il conviendrait de préciser et d'exposer davantage les fins pour lesquelles le traitement des données biométriques devrait être permis vu que le traitement des données biométriques constitue une ingérence particulièrement importante dans le droit à la protection de la personnalité de l'intéressé.

Paragraphes 5.6 et 5.7
5.6. Par contre, les paragraphes 5.6 et 5.7 pourraient être condensés.

Dans l'ensemble, il est à remarquer que le niveau de l'abstraction varie considérablement dans la Recommandation. Des ingérences particulièrement graves dans le droit à la protection de la personnalité (par exemple des mesures de surveillance, traitement des données biométriques) sont en partie traitées de manière plus courte et moins différenciée que les ingérences moins graves (par exemple l'usage des pages du réseau Internet ou Intranet). Même si cela n'est pas voulu, il conviendrait d'examiner ces questions et d'apporter des améliorations.

Paragraphe 12.2
Pour ce qui concerne le paragraphe 12.2, il n'est pas clair ce que signifie précisément l'expression « données à d'appréciation » (le cas échéant explication dans l'exposé des motifs).

Paragraphe 13.1
L'obligation prévue au paragraphe 13.1 de mettre régulièrement à jour des mesures techniques et organisationnelles imposera aux entreprises des charges qui ne pourront pas être appréciées dans toute leur envergure. Une évaluation de l'impact est suggérée à l'égard de ce sujet ainsi qu'à l'égard d'autres questions qui se manifestent dans des coûts causés à l'employeur ou aux entreprises.

BUREAU OF THE CDBI

I. Introduction ***(version française ci-après)***

At its 24th meeting (28-30 June 2011), the Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD-BUR) T-PD (June 2011) decided to communicate the draft Recommendation on the Protection of Personal Data Used for Employment Purposes to the Steering Committee on Bioethics for possible comments by 16 September 2011.
The CDBI delegations appreciated the opportunity to make comments on this draft Recommendation which addresses in particular the use of genetic data for employment purposes. This is indeed a very complex and sensitive issue, which was initially in the scope of the work undertaken by the CDBI with a view to the elaboration of a legal instrument on the applications of genetics in the health field as well as in the fields of insurance and employment. The CDBI started considering the applications in the field of health and decided, taking into account the progress made in the elaboration of the relevant provisions, to split the Protocol and to bring out separate instruments dealing with genetic testing for health purposes and genetic testing for insurance and for employment purposes. Work has already started on the applications in the field of insurance and a consultation paper is being elaborated on which T-PD has been invited to make comments. Even though this draft document addresses the field of insurance, many points raised in relation to genetic data, in particular in Chapter 2 are relevant when considering the use of genetic testing results in the field of employment. It also illustrates the complexity as well as the implications of the use of genetic data outside the health field which requires thorough analysis.

In the light of these considerations and as the time allowed for examination of a draft instrument received on 20 July 2011 which addresses some complex and sensitive issues, was very limited, the comments below should not be considered as a comprehensive opinion of the CDBI but only as preliminary comments from delegations.

The main comments presented below have been formulated in the light of CDBI's work carried out in particular in the field of genetics. Additional comments send by delegations on other aspects of the draft recommendation appear in appendix to this document.

II. Draft Recommendation on the on the Protection of Personal Data Used for Employment Purposes

The comments concern mainly Chapter 10 of the draft Recommendation dealing with particular categories of data.

A. General comments

Since the adoption of Rec(89)2 on the Protection of Personal Data Used for Employment Purposes, important scientific and technological developments have taken place, in particular in the field of genetics and information and communication technologies. The fact that the draft Recommendation submitted for comments takes into account these developments, is in general to be welcome.

Reference to the Convention on Human Rights and Biomedicine
Considering the bioethical issues raised by the use of genetic data outside the medical field, reference could be made in the preamble to the relevant provisions of the Convention on Human Rights and Biomedicine:

- Article 11 on the prohibition of discrimination on the basis of genetic heritage
- Article 12 prohibiting the performance of predictive genetic test for purposes other than health or scientific research linked to health purposes.

Genetic data
● An important change introduced in the draft Recommendation is a reference to "genetic data", which did not appear specifically in the Rec(89)2. The use of the expression "health data and genetic data" used in paragraphs 10.2 to 10.6, indicates a distinction between these two categories of data. "Genetic data" includes indeed health related data but also non health related data, (e.g. genetic fingerprints). If the intention of the drafters, as it seems to be the case, would be to focus on data relevant to health, it would seem therefore more appropriate to refer to "health data, including genetic data".

● Genetic data, as health related data, are sensitive personal data, calling for specific protective measures as acknowledged in the Recommendation. However, the predictive dimension of genetic data and the uncertainties which remain regarding the reliability of certain tests, the relevance and value of their results to anticipate future health of a person are to be duly taken into consideration when considering their potential use for employment purposes which may lead to discrimination. These points may deserve specific attention when defining the conditions to be fulfilled for exceptions to the general prohibition to collect and process genetic data for employment purposes (paragraph 10.2).

● Reference should be made in this context to the relevant sections of the Explanatory Report (ER) of the Convention on Human Rights and Biomedicine concerning Article 12. This Article only addresses the use of predictive genetic testing[6] and prohibits such use for other than health purposes or scientific research linked to health purpose. However, these paragraphs of the ER provide clarification with regard to the scope of the expression "health purposes" when it comes to the employment field. Furthermore, it identifies different benefits/interests and risks which are also at stake when considering the conditions for possible use for employment purposes of genetic data, previously obtained for another purpose – an issue which would deserve careful consideration.

> *"84. Because there is an apparent risk that use is made of genetic testing possibilities outside health care (for instance in the case of medical examination prior to an employment or insurance contract), it is of importance to clearly distinguish between health care purposes for the benefit of the individual on the one hand and third parties' interests, which may be commercial, on the other hand.*

[6] "Predictive genetic tests » refer to tests which are predictive of a monogenic disease, tests serving to detect a genetic predisposition or genetic susceptibility to a disease, or tests serving to identify the subject as a healthy carrier of a gene responsible for a disease. (Article 8.2 of the Additional Protocol concerning Genetic Testing for Health Purposes.

85. Article 12 prohibits the carrying out of predictive tests for reasons other than health or health-related research, even with the assent of the person concerned. Therefore, it is forbidden to do predictive genetic testing as part of pre-employment medical examinations, whenever it does not serve a health purpose of the individual. This means that in particular circumstances, when the working environment could have prejudicial consequences on the health of an individual because of a genetic predisposition, predictive genetic testing may be offered without prejudice to the aim of improving working conditions. The test should be clearly used in the interest of the individual's health. The right not to know should also be respected.

86. Insofar as predictive genetic testing, in the case of employment or private insurance contracts, does not have a health purpose, it entails a disproportionate interference in the rights of the individual to privacy."

87. However, national law may allow for the performance of a test predictive of a genetic disease outside the health field for one of the reasons and under the conditions provided for in Article 26.1 of the Convention."

Article 26 paragraph 1
"1. No restrictions shall be placed on the exercise of the rights and protective provisions contained in this Convention other than such as prescribed by law and are necessary in a democratic society in the interest of public safety, for the prevention of crime, for the protection of public health or for the protection of the rights and freedoms of others."

Extract of paragraph 149 of the Explanatory report related to Article 26.1
"149. [This Article] echoes partially the provisions of Article 8, paragraph 2, of the European Convention on Human Rights. The exceptions made in Article 8, paragraph 2, of the European Convention on Human Rights have not all been considered relevant to this Convention. The exceptions defined in the article are aimed at protecting collective interests (public safety, the prevention of crime, and the protection of public health) or the rights or freedoms of others."

These considerations are particularly relevant when considering in particular the provisions included in paragraph 10.2 of the draft Recommendation. Indeed, while points *a.* to *d.* do not raise particular problem[7], the added section dealing specifically with genetic data raised a number of questions starting with its interpretation but more substantially on content, which the CDBI has not discussed in depth. It is therefore not possible to take any position on such a complex and problematic issue that is the use of genetic data and more generally predictive health information (see also comment below: Other predictive data).

Other predictive data
● In the context of the work currently carried out by the CDBI on the use of genetic data in the field of insurance, it was acknowledged that other health data than genetic data may have predictive value. This is the case for example of the data resulting from X-Ray or other imaging technologies which may reveal the presence of signs which may be related to a possible disease which has not yet manifested (no symptoms).
The predictive value of such data may warrant, as this is the case for genetic data, special attention when considering their potential use for employments purposes.

● The issue of health data related to third parties is referred to in paragraph 10.7. One of the examples of third parties given is family members. Particular attention should be paid to the use of family history. Independently of the necessary safeguards for the protection of such sensitive data

[7] The Explanatory Memorandum should however specify that the expression « preventive medicine » includes occupational medicine.

and the issue of medical secrecy, potential use of such data for employment purposes raises also other ethical issues.
Paragraph 10.7 is referring to situation where such use would be made for the attribution of specific benefits. However, it could also be used for a decision in relation to the recruitment of a person (See case law in Germany as an example and ILO press communiqué referring to this case)[8]. Indeed health related data concerning family members (family history) of a potential employee may be collected considering that they could have a predictive value with regard to the future health of this person.
Such potential use should be taken into account and would require further analysis.

B. Additional specific remarks / proposals made by delegations in relation to genetic data and chapter 10

FRANCE
As regards the questions and reservations surrounding the certainty ascribed to certain predictive genetic data, the very idea of processing such data to determine the professional capacities of employees or applicants for employment raises very serious problems. This is why an extremely cautious approach must be taken to the idea of exceptions to the principle of prohibiting such processing.

Consequently, unless the T-PD were to agree to confine its draft to setting out a principle of prohibiting the collecting and processing of predictive data without exceptions, the French delegation proposes that the CDBI adopt a highly reserved position of principle on all the additions introducing issues relating to genetic data into Recommendation R (89) 2, considering that the withdrawal of these provisions would be the optimum solution in view of the unreadiness of this issue for consideration.

On a strictly subsidiary level, if the CDBI would find itself unable to implement the above proposals, the following amendments should be made to the draft text:

- In the last indent of para. *10.2*, the sentence "*Provision may be made for exceptions only within the limits laid down by domestic law and where there are appropriate safeguards, which should also provide for the prior involvement of the supervisory authorities, for the sole purpose of adopting, at the request of the employee, the measures necessary to improve his health, safety and working conditions"* should be amended as follows:

  If, on an exceptional basis, States were to provide for exceptions to this principle in their domestic law, accompanied by appropriate safeguards and in conformity with international law on personal data protection, such exceptions should be submitted in advance to these States' data protection authorities and be geared solely to adopting, at the request of the employee, the measures necessary to improve his health, safety and working conditions";

- In paras. *10.3* and *10.4*, the words "*where their processing is lawful, genetic data* (etc)" should be replaced by the words "*where their processing is authorised by national law in conformity with international law on personal data protection, genetic data* (etc)";

[8] Verwaltungsgericht Darmstadt: Case Number: 1 E 470/04 – 24 June 2004
http://www.lareda.hessenrecht.hessen.de/jportal/portal/t/17cz/page/bslaredaprod.psml/js_pane/Dokumentanzeige#focuspoint
ILO press release 9 May 2007: http://www.ilo.org/global/about-the-ilo/press-and-media-centre/news/WCMS_082589/lang--en/index.htm

- The current wording of para. *10.3* to the effect that "*health data and, where their processing is lawful, genetic data, may not be collected from sources other than the employee concerned except with his express and informed consent or in accordance with provisions of domestic law*", would appear, because of the words "*or in accordance with provisions of domestic law*", incompatible with the principle set out at the end of para. 10.2 to the effect that genetic data can only be processed in derogation of the prohibition principle at the request of the employee. The words "*or in accordance with provisions of domestic law*" should therefore be deleted.

Moreover, in specific connection with genetic data, it would be very difficult and disputable to allow, by extending the scope of the provision which was included in Recommendation 89 (2), health data covered by medical secrecy to be communicated to members of a personnel department not bound by such secrecy with a view to decision-making by the latter. This option is liable to important abuses including in particular discriminatory treatment of specific employees on the basis of disclosure of predictive data. It should therefore be deleted.

Lastly, irrespective of the problems raised by introducing genetic data into the Recommendation, the new principle set out in para. *10.7* concerning the possibility for the employer, in certain cases, to process health data relating to third parties, such as members of the employee's family, requires much stricter regulation, particularly in the light of Article 6 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (regulating the processing of sensitive data such as personal data concerning health). As the draft stands, the bare mention in the explanatory memorandum of examples which are to be quoted for information is insufficient to guarantee such regulation. If such personal data processing in derogation of medical secrecy proves necessary to specific States for purposes such as establishing entitlement to special benefits, prior mention would be needed of the principle of prohibiting the processing of health data on third parties, followed by a provision on a possible exception confined to one specific, explicit purpose set out in the text of the appendix to the Recommendation, rather than in the explanatory memorandum.

IRELAND

Para 10.3 - It is suggested that processing of genetic data for employment purposes should only be permitted where the prior approval of the national data protection authority has been obtained and subject to such conditions as may be applied by that authority in any particular case and where any other legal obligation has been met. In other words that even express consent of individuals should not be enough to permit such processing. This position is somewhat reflecting in the accompanying commentary to para 10.2.

Para 10.6 - Is it that where a data subject's right of access to his health data could cause serious harm to the data subject that such data may be communicated 'to' rather than "through" a medical practitioner for the purpose of assessing whether disclosure of the data will impact on the data subject? This is not as clear as it might be. Also is it appropriate that the employee chooses the doctor who makes the decision as to the potential impact of the health data on the data subject? Why can the employer not choose this practitioner? Finally how is serious harm to be defined?

NORWAY

The Norwegian delegation has following comments to the draft recommendation on the protection of personal data used for employment purposes. Our comment concerns *art 10.2 second paragraph*:

The Norwegian Act relating to the application of biotechnology in medicine article 5-8 clearly prohibits the use of predictive genetic information outside the health service. This includes

requesting, receiving, being in possession of or using of such information. Genetic predictive information is defined as “pre-symptomatic genetic testing, predictive genetic testing, and testing to determine whether or not a person is a carrier of hereditary disease that will only be expressed in later generations (carrier testing)” and also includes information deriving from systematic surveys of hereditary disease within a family. Since the draft recommendation in principle prohibits the collection and use of genetic information for employment purposes, and an exemption form this principle must be clearly stated and limited in national law, Norwegian legislation will not be in breach with this due to the clear prohibition in Norwegian law. As we read the draft, it is not a prerequisite to legislate nationally such an exemption as suggested in the draft recommendation.

APPENDIX

Comments on other chapters of the draft Recommendation sent by CDBI Delegations

IRELAND

General Comments

The document comprehensively deals with the issue of processing personal data for employment purposes. It is particular welcome that issues arising in the context of ICT e.g. monitoring internet usage by employees are addressed in the draft Recommendation.

The Recommendation deal with the collection and processing (section 5), storage (Section 6), use (Section 7) and conservation of data (Section 14). However, the issue of whether and under what circumstances data should be destroyed is not explicitly addressed in the current draft. Section 14 touches on the issue by reference to conservation of data and does refer to deletion of data of unsuccessful job applicants. No specific reference however is made to current employees and their rights in relation to stored data once they have left employment.

Specific Comments

Para 3.1- it is not clear who 'certifies' the information and technology systems referred to in this paragraph

Para 5.3- It is difficult to see how this recommendation could be enforced. Moreover, it could be argued that if an individual voluntarily posts information about themselves on a social or professional networking site, they must be aware that the information will be available to third parties including potential employers. Thus, the recommendation could be considered overly restrictive. It does however need to be recognised, that in the absence of a “right to be forgotten” there is a danger that previous infractions by a younger self recorded by social media sites could have deleterious implications for employment. It should be considered whether this recommendation is the appropriate forum for dealing with that eventuality.

Para 5.7 - there is an assertion here that access to personal e mails of the employee should "never be permitted"- I wonder is this too extreme - could there not be circumstances where access could reasonably be required?

Para 6.2 - By providing an inherent link to a given individual’s identity, biometric information could potentially be used for numerous different purposes beyond just recognition. Thus, the draft recommendation that as a rule biometric data should not be stored in databases goes some way to mitigating the potential for function creep. Verification-based systems enable an individual to retain control over his/her biometric information because his/her template can be stored locally (*e.g.* on a smart card) and not in a centralised database, thereby, providing better safeguards for privacy.

Para 7.2 - it is not clear what this paragraph is saying, further clarification required

Para 9.3 - it would be helpful if specific examples were given in relation to when the consent of an employee may be required as a safeguard.

Para 12.1 - it is not clear what is meant by referring to the introduction of “general *preventative* procedures to ensure that there is an adequate and prompt response" where employees seek access to the information about them which is stored by their employer

Para14.4 - it is not clear what is meant by the phrase " in due time".

ITALY

The Italian delegation, in agreement with and sharing the satisfaction of the Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), wishes to recall that Convention CETS No. 108 of 1981 was ratified by Italy on 29 March 1997 and was already in force as from 1 July 1997. Upon accession to the Convention, provision was made in Italy for setting up the “Ufficio del Garante” (Office for the protection of human rights with regard to the processing of personal data) for the purpose of issuing recommendations and binding opinions concerning the real application of protection of individuals and data and resolving controversial issues.

The Italian delegation, in agreement with the initiative taken by the CDBI to carry out monitoring of the bioethical aspect of the Convention’s implementation in the various Council of Europe member countries, wishes to stress that where Italy is concerned, a more specific appraisal of “Draft Recommendation CM/REC(2011) of the Committee of Ministers on the protection of personal data used for employment purposes” also comprises the expression of the opinion of the “Garante”, whose function was confirmed by the “Codice in materia di protezione dei dati personali” adopted by Decreto Legislativo No. 196 of 30 June 2003, referring to every form of regulation of personal data in all circumstances, above and beyond those relating to the use of computer resources and the aim of processing for employment purposes.

It should also be recalled that, with particular regard to the processing of genetic data, there was an update in this area on 24 June 2011 with Opinion No. 258 “Autorizzazione generale al trattamento dei dati genetici” (general authorisation for processing genetic data), published in the Gazzetta Ufficiale della Repubblica italiana, general series no. 159 of 11 July 2011.

SPAIN

We are in agreement with the document. Two comments:

- In *Section 6.2*, the wording of the second paragraph is difficult to understand. The first question is: How can a biometric identification be carried out without a reference database? A possible answer suggested by the text is by coding the biometric data and make them available in a media (e.g., an "intelligent" card) to the person concerned. A possible problem we see here is that identification is no longer based on the real biometric data, but just on a matching between some biometric data and the data stored in a card. It's no longer a biometric identification in strict sense. The storage media may be stolen or duplicated and used to supplant the person concerned (the only requirement now is matching data) who may find it difficult to prove that "it wasn't me".

- In *Section 9.3*, we suggest to modify the sentence "the consent of the employee may also be required as safeguard" by the following: “the consent of the employee should be required as safeguard”.

I. Introduction

Lors de sa 24e réunion (28-30 juin 2011), le Bureau du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a décidé de transmettre au Comité directeur pour la bioéthique le projet de Recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi, en vue de recueillir d'éventuelles observations pour le 16 septembre 2011.

Les délégations du CDBI ont apprécié la possibilité qui leur a été donnée de formuler des remarques sur ce projet de Recommandation, qui traite en particulier de l'utilisation de données génétiques à des fins d'emploi.

Il s'agit en effet d'une question très complexe et délicate, qui entrait initialement dans le cadre des travaux menés par le CDBI en vue de l'élaboration d'un instrument juridique sur les applications de la génétique dans le domaine de la santé, ainsi que dans le domaine des assurances et de l'emploi. Le CDBI a commencé à examiner les applications dans le domaine de la santé et a décidé, compte tenu des progrès réalisés dans l'élaboration des dispositions pertinentes, de scinder le Protocole et de publier des instruments distincts traitant des tests génétiques à des fins de santé, des tests génétiques à des fins d'assurance et des tests génétiques à des fins d'emploi. Les travaux portant sur les applications dans le domaine des assurances ont déjà débuté, et un document de consultation est en cours d'élaboration – document sur lequel le T-PD a été invité à formuler des observations. Bien que ce projet de document traite du domaine des assurances, de nombreux points soulevés au sujet des données génétiques, notamment au chapitre 2, sont également pertinents lorsque l'on examine la question de l'utilisation des résultats de tests génétiques dans le domaine de l'emploi. Ce document illustre également la complexité et les implications de l'utilisation de données génétiques en dehors du domaine de la santé, autant de questions qui méritent une analyse approfondie.

A la lumière de ces considérations, et compte tenu du délai très court accordé pour l'examen du texte précité reçu le 20 juillet 2011, qui traite de questions complexes et sensibles, les observations ci-dessous ne doivent pas être considérées comme un avis finalisé du CDBI, mais comme des observations préliminaires formulées par les délégations.

Les principales remarques présentées ci-après ont été formulées à la lumière des travaux menés par le CDBI, notamment dans le domaine de la génétique.

D'autres commentaires envoyés par les délégations sur d'autres aspects du projet de recommandation figurent en annexe du présent document.

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

Les commentaires portent principalement sur le chapitre 10 du projet de recommandation, traitant de catégories particulières de données.

A. Observations générales

Depuis l'adoption de la Rec(89)2 sur la protection des données à caractère personnel utilisées à des fins d'emploi, d'importants développements scientifiques et technologiques ont eu lieu, notamment dans le domaine de la génétique et des technologies de l'information et de la

communication. Il convient de se féliciter, de manière générale, de la prise en considération de ces développements dans le projet de recommandation soumis pour commentaires.

Référence à la Convention sur les droits de l'homme et la biomédecine
Compte tenu des questions de bioéthique soulevées par l'utilisation de données génétiques en dehors du domaine médical, le préambule pourrait faire référence aux dispositions pertinentes de la Convention sur les droits de l'homme et la biomédecine :

- Article 11 interdisant toute discrimination en raison du patrimoine génétique
- Article 12 interdisant la réalisation de tests génétiques prédictifs à des fins autres que médicales ou de recherche médicale.

Données génétiques
● Une modification importante introduite dans le projet de Recommandation est la référence aux « données génétiques », qui n'apparaissait pas spécifiquement dans la Rec(89)2. L'expression « données de santé et données génétiques » utilisée aux paragraphes 10.2 à 10.6 indique qu'une distinction est faite entre ces deux catégories de données. Les « données génétiques » incluent en effet des données de santé, mais également d'autres données non liées à la santé (par exemple empreintes génétiques). Si, comme cela semble être le cas, l'intention des rédacteurs est de mettre l'accent sur les données pertinentes pour la santé, il semblerait plus approprié d'écrire « les données de santé, y compris les données génétiques ».

● Les données génétiques, tout comme les données liées à la santé, sont des données à caractère personnel sensibles qui nécessitent des mesures de protection spécifiques, comme le reconnaît la Recommandation. Toutefois, la dimension prédictive des données génétiques et les incertitudes qui subsistent quant à la fiabilité de certains tests, ainsi que la pertinence et la valeur de leurs résultats pour anticiper l'état de santé futur d'une personne doivent être dûment prises en compte lorsque l'on examine leur utilisation potentielle à des fins d'emploi, celle-ci pouvant être source de discrimination. Ces points mériteraient une attention particulière lors de la définition des conditions à remplir pour les dérogations à l'interdiction générale de collecter et de traiter des données génétiques à des fins d'emploi (paragraphe 10.2).

● Il convient de faire référence, dans ce contexte, aux paragraphes du rapport explicatif (RE) de la Convention sur les droits de l'homme et la biomédecine relatifs à l'article 12. Cet article porte uniquement sur l'utilisation de tests génétiques prédictifs[9] et qu'il interdit à des fins autres que médicales ou de recherche médicale. Néanmoins, les paragraphes du RE en question précisent le champ d'application de l'expression « à des fins médicales » lorsqu'il s'agit du domaine de l'emploi. En outre, ils identifient les différents bénéfices/intérêts et risques qui sont également en jeu lorsque l'on envisage l'utilisation éventuelle à des fins d'emploi de données génétiques précédemment obtenues à une autre fin – une question qui nécessite d'être examinée avec soin.

> *« 84. Parce qu'il y a un risque apparent d'usage des possibilités de tests génétiques en dehors des soins de santé (par exemple en cas d'examen médical avant un contrat d'emploi ou d'assurance), il est important de distinguer clairement entre les raisons de soins de santé pour le bénéfice de l'individu, d'une part, et les intérêts de tiers, qui peuvent être commerciaux, de l'autre.*
>
> *85. L'article 12 interdit d'entreprendre, même avec l'assentiment de la personne concernée, un test prédictif pour une raison autre que médicale ou de recherche médicale. Il est donc exclu de réaliser des tests génétiques prédictifs dans le contexte d'examens médicaux de pré-embauche*

[9] Les « tests génétiques prédictifs » désignent les tests prédictifs de maladies monogéniques, les tests permettant de détecter une prédisposition génétique ou une susceptibilité génétique à une maladie ou les tests permettant d'identifier le sujet comme porteur sain d'un gène responsable d'une maladie. (Article 8.2 du Protocole additionnel relatif aux tests génétiques à des fins médicales).

chaque fois qu'ils ne poursuivent pas un but de santé pour la personne concernée. Cela signifie que, dans des circonstances particulières, lorsque les conditions de travail pourraient avoir des conséquences préjudiciables pour la santé d'une personne en raison de sa prédisposition génétique, des tests génétiques prédictifs pourraient être proposés, sans préjudice de l'objectif d'améliorer le cadre du travail. Les tests doivent être clairement utilisés dans l'intérêt de la santé de l'intéressé. Son droit de ne pas être informé doit être respecté.

86. Dans la mesure où les tests prédictifs, dans le cas des contrats d'assurance privés ou d'emploi, ne tendent pas à un objectif sanitaire, ils comportent une atteinte disproportionnée aux droits de l'individu ou au respect de la vie privée ».

Article 26 paragraphe 1

« 1. *L'exercice des droits et les dispositions de protection contenus dans la présente Convention ne peuvent faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sûreté publique, à la prévention des infractions pénales, à la protection de la santé publique ou à la protection des droits et libertés d'autrui. »*

Extrait du Rapport explicatif concernant l'Article 26 paragraphe 1

« 149. [Cet article] reprend quelques-unes des restrictions figurant à l'article 8, paragraphe 2, de la Convention européenne des Droits de l'Homme. Les exceptions visées au paragraphe 2 de l'article 8 de la Convention européenne des Droits de l'Homme n'ont cependant pas toutes été considérées comme pertinentes aux fins de la présente Convention. Les exceptions que l'article définit sont fondées sur la protection d'intérêts collectifs (sûreté publique, prévention des infractions pénales, protection de la santé publique) ou encore sur la protection des droits et libertés d'autrui. »

Ces considérations sont particulièrement pertinentes lorsque l'on examine notamment les dispositions figurant au paragraphe 10-2 du projet de Recommandation. En effet, si les points *a.* à *d*. ne posent pas de problème particulier[10], la section nouvellement insérée traitant spécifiquement des données génétiques soulève un certain nombre de questions, à commencer par son interprétation, mais surtout quant à sa teneur, que le CDBI n'a pas examinées en profondeur. Il n'est donc pas possible de prendre position sur une question aussi complexe et difficile que celle de l'utilisation de données génétiques et plus généralement des informations prédictives liées à la santé (voir également commentaires ci-dessous : Autres données prédictives).

Autres données prédictives

● Dans le cadre des travaux menés actuellement par le CDBI sur l'utilisation des données génétiques dans le domaine des assurances, il a été reconnu que des données de santé autres que les données génétiques peuvent avoir une valeur prédictive. Tel est le cas, par exemple, des données résultant de radiographies ou d'autres techniques d'imagerie susceptibles de révéler la présence de signes pouvant être liés à une éventuelle maladie ne s'étant pas encore manifestée (absence de symptômes).

La valeur prédictive de ces données mériterait, comme c'est le cas pour les données génétiques, une attention particulière lors de l'examen de leur utilisation potentielle à des fins d'emploi.

[10] L'exposé des motifs devrait toutefois préciser que l'expression "médecine préventive" inclut la médecine du travail.

● La question des données de santé relatives à des tiers est évoquée au paragraphe 10.7. Les membres de la famille figurent parmi les exemples de tiers qui sont donnés dans le texte. Une attention particulière devrait être portée à l'utilisation des antécédents familiaux (histoire familiale). Abstraction faite des garanties nécessaires pour la protection de ces données sensibles et de la question du secret médical, l'utilisation potentielle de ces données à des fins d'emploi soulève également d'autres questions éthiques.

Le paragraphe 10.7 évoque une situation dans laquelle une telle utilisation serait faite en vue de l'attribution de prestations spécifiques. Toutefois, ces données pourraient également servir à prendre une décision concernant le recrutement d'une personne (voir à titre d'exemple la jurisprudence allemande et le communiqué de presse de l'OIT concernant cette affaire)[11]. En effet, les données de santé concernant la famille d'un candidat à l'embauche (histoire familiale) pourraient être recueillies en considérant qu'elles pourraient avoir une valeur prédictive quant à l'état de santé futur de cette personne.

Cette utilisation potentielle devrait être prise en compte et mériterait une analyse plus poussée.

B. Remarques spécifiques / propositions faites par les délégations relatives aux données génétiques et au chapitre 10

FRANCE
Eu égard aux interrogations et aux réserves dont fait l'objet le caractère de certitude prêté à certaines données génétiques prédictives, l'idée même d'un traitement de telles données pour déterminer l'aptitude professionnelle des employés ou des candidats à l'emploi s'avère profondément problématique. C'est pourquoi l'idée de dérogations au principe d'interdiction de ces traitements doit être abordée avec la plus extrême précaution.

En conséquence, sauf à ce que à ce que le T-PD accepte de se borner à énoncer dans son projet un principe d'interdiction de collecte et de traitement des données prédictives, non assorti de dérogations, la délégation française propose au CDBI d'adopter une position de principe très réservée quant à l'ensemble des adjonctions introduisant les problématiques relatives aux données génétiques dans la recommandation R (89)2, un retrait de ces dispositions apparaissant, en l'état de maturation insuffisante qui est celui de cette question, comme la solution la plus opportune.

A titre très subsidiaire, s'il s'avérait que les propositions formulées ci-avant ne peuvent être mises en œuvre par le CDBI, il conviendrait d'introduire dans le texte du projet les modifications suivantes :

- Au dernier alinéa du point 10.2, la phrase selon laquelle *« 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 préventive 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. »* devrait être ainsi amendée :

[11] Verwaltungsgericht Darmstadt: Affaire numéro : 1 E 470/04 – 24 juin 2004
http://www.lareda.hessenrecht.hessen.de/jportal/portal/t/17cz/page/bslaredaprod.psml/js_pane/Dokumentanzeige#focuspoint
Communiqué de presse de l'OIT du 9 mai 2007 : http://www.ilo.org/global/about-the-ilo/press-and-media-centre/news/WCMS_082589/lang--en/index.htm

« Si, à titre exceptionnel, des Etats prévoyaient dans leur droit interne, dans le cadre de garanties appropriées et en conformité avec le droit international de la protection des données à caractère personnel, des dérogations à ce principe, celles-ci devraient être préalablement soumises aux autorités de contrôle en matière de protection des données de ces Etats et avoir pour unique objectif d'adopter, à la demande de l'employé, les mesures nécessaires à son état de santé, ou à ses conditions de sécurité ou de travail. » ;

- Aux points 10.3 et 10.4, les mots *« lorsque leur traitement est licite, les données génétiques…etc… »* devraient se voir substituer les *mots « lorsque leur traitement est autorisé par le droit national en conformité avec le droit international de la protection des données à caractère personnel, les données génétiques…etc…»* ;

- La rédaction actuelle du 10.3, selon laquelle *« 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 »*, apparaît, du fait des mots *« ou conformément aux dispositions du droit interne »*, en contradiction avec le principe énoncé à la fin du point 10.2, selon lequel un traitement de données génétiques dérogeant au principe d'interdiction ne peut être mis en œuvre qu'à la demande de l'employé. Il conviendrait donc de supprimer au 10.3 le mot *« ou conformément aux dispositions du droit interne »* ;

Par ailleurs, et s'agissant en particulier s'agissant des données génétiques, il paraît très délicat et contestable d'admettre, par une extension de la portée de la disposition qui figurait dans la recommandation 89(2) que des données de santé couvertes par le secret médical puissent être communiquées à des membres du service du personnel non liés par ce secret en vue de la prise de décisions par ce service. Une telle possibilité pourrait autoriser de graves dérives, consistant en particulier dans des traitements discriminatoires de certains employés sur la base de la communication de données prédictives. Elle doit donc être supprimée.

Enfin, indépendamment des problèmes que pose l'introduction dans la recommandation des données génétiques, le principe nouveau posé au point 10.7, relatif à la possibilité pour l'employeur de traiter dans certains cas des données de santé relatives à des tiers tels que des membres de la famille de l'employé appelle un encadrement beaucoup plus strict, en particulier au regard de l'article 6 de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard des traitements de données à caractère personnel (encadrement des traitements de données sensibles, tels ceux de données relatives à la santé des personnes). En effet, en l'état de la rédaction, la simple mention dans l'exposé des motifs de certains exemples qu'il est envisagé d'y citer à titre indicatif ne suffit pas à garantir cet encadrement. S'il s'avère que de tels traitements de données à caractère personnel, en dérogation au secret médical, est nécessaire pour certains Etats dans le cadre de finalités telles que l'octroi de prestations spécifiques, il conviendrait d'énoncer d'abord un principe d'interdiction des traitements de données de santé relatives à des tiers, puis de prévoir une possibilité de dérogation circonscrite à une finalité déterminée et explicite, mentionnée dans le texte même de l'annexe de la recommandation, et non pas dans l'exposé des motifs.

IRLANDE

Par. 10.3 : Ce point laisse entendre que le traitement des données génétiques à des fins d'emploi ne devrait être permis que si l'autorité nationale chargée de la protection des données a donné son accord préalable, sous réserve des conditions dont cette autorité peut assortir le cas particulier et de toutes autres dispositions légales applicables. En d'autres termes, même le consentement

exprès des intéressés ne suffirait pas pour permettre ce traitement. Cette position est reflétée d'une certaine manière dans les observations qui accompagnent le point 10.2.

Par. 10.6 : Est-ce parce que le droit d'accès de la personne concernée à ses données médicales pourrait conduire à « porter une grave atteinte » à celle-ci que ces données peuvent être communiquées à un médecin de son choix (plutôt que « par l'intermédiaire» de celui-ci) afin qu'il évalue l'effet que cette divulgation de données pourrait avoir sur l'intéressé ? Ce n'est pas aussi clair que cela pourrait l'être. Convient-il aussi que ce soit l'employé qui choisisse le médecin responsable de la décision quant à l'effet éventuel des données de santé sur la personne concernée ? Pourquoi l'employeur ne pourrait-il pas choisir le médecin ? Enfin, comment définir « grave atteinte » ?

NORVÈGE

La délégation norvégienne souhaite formuler les commentaires suivants au sujet du Projet de recommandation sur la protection des données à caractère personnel utilisées à des fins d'emploi. Nos commentaires portent sur le deuxième paragraphe de l'article 10.2 :

L'article 5-8 de la loi norvégienne relative à l'application de la biotechnologie en médecine interdit expressément l'utilisation d'informations génétiques prédictives en dehors du cadre des services de santé. Cette interdiction inclut le fait de demander, de recevoir, de posséder ou d'utiliser des informations de cette nature. Sont considérées comme des informations génétiques prédictives « les tests génétiques pré symptomatiques, les tests génétiques prédictifs et les tests destinés à déterminer si une personne est ou non porteuse d'une maladie héréditaire qui ne s'exprimera que dans les générations ultérieures (test de porteur sain) » ainsi que les informations provenant d'études systématiques de maladies héréditaires au sein d'une famille. Etant donné que le projet de recommandation interdit en principe la collecte et l'utilisation d'informations génétiques à des fins d'emploi et que toute dérogation à ce principe doit être exceptionnelle et dans les seules limites prévues par le droit interne, la législation norvégienne sera conforme à ces dispositions puisqu'elle énonce une interdiction claire à cet égard. Selon la lecture que nous faisons du projet, il n'est pas obligatoire que le droit interne prévoie les dérogations envisagées par le projet de Recommandation.

ANNEXE

Commentaires sur d'autres chapitres du projet de Recommandation envoyés par les délégations du CDBI

IRLANDE

Généralités
Le document examine en détail la question du traitement des données à caractère personnel utilisées à des fins d'emploi. Il est particulièrement approprié que les questions soulevées par les TIC comme la surveillance de l'usage d'Internet que font les employés, soient abordées dans le projet de Recommandation.

La recommandation concerne la collecte et le traitement (partie 5), l'enregistrement (partie 6), l'utilisation interne (partie 7) et la conservation des données (partie 14). Cependant, le projet actuel ne s'intéresse pas expressément à la question de savoir si les données devraient être ou non détruites et dans quelles circonstances. La section 14 approche la question en traitant de la conservation des données et évoque la suppression des données relatives aux candidats à un emploi non retenus. Cependant, aucune mention n'est faite des employés en cours de contrat, ni de leurs droits par rapport aux données enregistrées une fois qu'ils ont quitté leur emploi.

Observations spécifiques
Par. 3.1 : On ne sait pas bien qui « certifie » les systèmes et technologies d'information visés dans ce paragraphe.

Par. 5.3 : Il est de difficile de savoir comment cette recommandation pourrait être mise en œuvre. De plus, on peut soutenir que si une personne publie volontairement des informations qui la concernent sur un site de réseautage social ou professionnel, elle doit être consciente que les informations seront accessibles à des tiers, y compris des employeurs éventuels. C'est pourquoi, la recommandation pourrait être considérée comme trop restrictive. Il convient toutefois de reconnaître qu'en l'absence d'un « droit à l'oubli », il est à craindre que des infractions commises par le passé et enregistrées sur un site de réseau social nuisent aux perspectives d'emploi de l'intéressé. Il importerait de se demander si la recommandation est le moyen approprié pour traiter ce cas de figure.

Par. 5.7 : Ce point indique que l'accès aux messages personnels d'un employé « ne peut être permis » - je me demande si ce n'est pas aller trop loin. N'y a-t-il pas des circonstances où l'accès pourrait raisonnablement être exigé ?

Par. 6.2 : En prévoyant un lien intrinsèque avec l'identité d'une personne, les informations biométriques qui la concernent pourraient être exploitées dans des buts bien différents de la simple reconnaissance de celle-ci. C'est pourquoi, le projet de Recommandation selon lequel les données biométriques ne devraient pas, en principe, être enregistrées dans une base de données contribue dans une certaine mesure à réduire le risque d'un détournement fonctionnel. Les systèmes supposant une vérification permettent aux particuliers de conserver la maîtrise de leurs données biométriques, car leur gabarit peut être conservé localement (par ex. sur une carte à mémoire) et non dans une base de données centralisée, ce qui offre des garanties de respect de la vie privée.

Par. 7.2 : On ne sait pas bien ce que ce point veut dire ; il demanderait à être précisé.

Par. 9.3 : Il serait utile de donner des exemples spécifiques où, par précaution, le consentement de l'employé devrait être requis.

Par. 12.1 : On ne sait pas bien ce que signifie « procédures préventives d'ordre général afin de garantir que le contrôle soit adéquat et rapide » au cas où des employés demandent à avoir accès aux informations les concernant qui sont conservées par leur employeur.

Par. 14.4 : On ne sait pas bien ce que signifie l'expression « dans les meilleurs délais ».

ITALIE
La Délégation italienne en accord et se félicitant avec le Bureau du Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n.108) veut rappeler que la Convention STCE n° 108 de 1981 a été ratifiée par l'Italie le 29 du mois de mars 1997 et est en vigueur depuis le 1er juillet 1997. Avec l'adhésion à la Convention, on a prévu l'institution en Italie de l' "Ufficio del Garante" (Bureau chargé de la protection des droits de la personne au regard du traitement des données personnelles) avec le but de donner des recommandations et des avis contraignants pour ce qui concerne la réelle application de la protection des personnes et des données et de résoudre les controverses.

La Délégation italienne, en accord avec l'initiative prise par le CDBI de suivre l'impact, en matière de bioéthique, de l'application de la Convention dans les différents Etats membres du Conseil de l'Europe, souligne que l'Italie souhaite une évaluation plus spécifique du "Projet de Recommandation CM/REC(2011) du Comité des Ministres sur la protection de données à caractère personnel utilisées à des fins d'emploi" et comporte aussi l'expression de l'opinion du Garant pour la protection des données personnelles, dont la fonction a été confirmée par le "Codice in materia di protezione dei dati personali" adopté par le Decreto Legislativo 30 giugno 2003, n. 196, qui se réfère à toute forme de règlementation et circonstance relatives aux données personnelles, ainsi qu'à l'utilisation des moyens informatiques aux fins d'emploi.

Il faut aussi rappeler qu'en ce qui concerne le traitement des données génétiques, une mise à jour a été effectuée le 24 juin 2011 avec l'avis n° 258 "Autorizzazione generale al trattamento dei dati genetici" (Autorisation générale au traitement des données génétiques), publiée par la Gazzetta Ufficiale della Repubblica italiana, Serie generale 11 luglio 2011, n. 159.

ESPAGNE
Nous sommes d'accord avec ce document. Deux commentaires :

- À l'article 6.2, la formulation du deuxième paragraphe est difficile à comprendre et pourrait être mal interprétée. La première question est celle de savoir comment une identification biométrique peut-elle être effectuée sans une base de données de référence. Une réponse possible suggérée pour le texte est : en codant les données biométriques et en les communiquant sur un support (par exemple, une carte « intelligente ») à la personne concernée. Un problème éventuel que nous voyons ici est que l'identification n'est plus basée sur des données biométriques réelles, mais juste sur une correspondance entre des données biométriques et les données stockées sur la carte. Il ne s'agit plus d'une identification biométrique à proprement parler. Le support de stockage peut être volé ou dupliqué et utilisé à la place de la personne concernée qui peut alors avoir des difficultés à prouver que « ce n'est pas moi » (la seule nécessité étant alors une correspondance de données).

À l'article 9.3, nous suggérons de remplacer la phrase « le consentement de l'employé peut aussi être requis » par la suivante « le consentement de l'employé devrait être requis ».