



**5062/01 FR/Final
WP 48**

Avis 8/2001

sur le traitement des données à caractère personnel
dans le contexte professionnel

Adopté le 13 septembre 2001

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE. Le secrétariat est assuré par:

la Commission européenne, DG Marché intérieur, unité "Fonctionnement et impact du marché intérieur; coordination; protection des données".

Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgique - Bureau: C100-6/136

Téléphone : ligne directe (+32-2)295.72.58 ou 299.27.19, centrale 299.11.11. Fax : 296.80.10

Adresse Internet : http://europa.eu.int/comm//internal_market/fr/dataprot/wpdocs/index.htm

LE GROUPE DE PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995¹,

vu les articles 29 et 30, paragraphes 1 (a) et 3 de la directive précitée,

vu son règlement intérieur, et notamment les articles 12 et 14 de ce dernier,

a adopté le présent avis:

1. Introduction

Le traitement des données à caractère personnel dans le contexte professionnel est sujet à débat tant au niveau communautaire que national.

Les gouvernements et les autorités de contrôle des États membres ont établi ou sont en passe d'établir une législation, des codes, des recommandations et réalisent des études abordant plusieurs aspects relatifs à la protection des données dans le contexte professionnel.

Travaux en cours et initiatives récentes:

BELGIQUE	<i>Avis n° 10/2000 de la Commission de la protection de la vie privée “Avis d’initiative relatif à la surveillance par l’employeur de l’utilisation du système informatique sur le lieu de travail”²</i>
FRANCE	<i>Rapport de consultation publique de la CNIL “La cybersurveillance des salariés dans l’entreprise”³</i>
GRECE	<i>Projet de recommandation sur la protection des données relatives aux employés⁴</i>

¹ Journal officiel n° L 281 du 23/11/1995, p. 31, disponible à l'adresse suivante:
http://europa.eu.int/comm/internal_market/fr/media/dataprot/index.htm

² www.privacy.fgov.be

³ www.cnil.fr/thematic/indextd2.htm

⁴ www.dpa.gr (seulement en grec)

ALLEMAGNE	<i>Le Parlement a demandé à maintes reprises au Gouvernement de présenter un projet de loi concernant la protection des données à caractère personnel dans les relations professionnelles.</i>
PAYS-BAS	<i>Rapport de la Registratiekamer "Working Well in Networks"⁵</i>
ESPAGNE	<i>Étude publiée par l'Agence espagnole de protection des données "Utilisation et contrôle des données automatisées dans le milieu professionnel"⁶.</i>
ROYAUME-UNI	<i>Projet de code de pratiques du Commissaire à l'information "Utilisation des données à caractère personnel dans les relations employé/employeur"⁷</i>

Les autorités de contrôle ont régulièrement traité toute une série de problèmes relatifs à la protection des données à caractère personnel dans le contexte professionnel, notamment:

- ❑ l'exactitude des données concernant le personnel
- ❑ le contrôle de l'utilisation du téléphone à des fins personnelles
- ❑ l'accès aux informations médicales
- ❑ l'utilisation d'informations relatives à l'appartenance syndicale
- ❑ le traitement au cours de fusions ou acquisitions d'entreprises

Les lois relatives à la protection de données à caractère personnel dans l'Union européenne confèrent des droits individuels à toute personne concernée par le traitement de ces données (p. ex.: droit d'accès, droit de rectification). En règle générale, ces droits s'appliquent intégralement à la relation employeur/employé et les seules exceptions possibles sont celles autorisées par la directive 95/46/CE. Toutefois, en raison du caractère relativement général de la directive, une orientation sera la bienvenue pour clarifier certains aspects de l'application des dispositions susmentionnées dans le contexte professionnel.

⁵ www.cbpweb.nl

⁶ non disponible sur le Web; contactez: Agencia de Protección de Datos. C/Sagasta 22, 28004, Madrid

⁷ wood.ccta.gov.uk/dpr/dpdoc.nsf

Dans le cadre de l'agenda pour la politique sociale, la Commission européenne a lancé une procédure de consultation des partenaires sociaux sur la protection des données dans le contexte professionnel.

Pour contribuer à l'application uniforme des mesures nationales adoptées au titre de la directive 95/46/CE, le groupe de travail a mis sur pied un sous-groupe pour examiner cette question⁸ et adopter le présent avis.

Actuellement, ce sous-groupe travaille sur un avis spécifique qui se concentrera sur l'application de la directive 95/46/CE en matière de surveillance et de contrôle des communications électroniques sur le lieu de travail.

2. Traitement de données à caractère personnel sur le lieu de travail

Employeurs et travailleurs doivent savoir que bon nombre d'activités courantes qui se déroulent dans le contexte professionnel engendrent le traitement de données à caractère personnel relatives aux travailleurs, parfois d'une sensibilité extrême.

En réalité, les employeurs rassemblent des données à caractère personnel relatives à leurs travailleurs à différentes fins depuis le commencement de la relation professionnelle, voire avant. Pendant le processus de recrutement, les candidats à un poste doivent fournir des informations personnelles à leur employeur potentiel qui, en même temps, traite généralement ces informations personnelles pour évaluer les compétences des candidats.

La collecte et le traitement ultérieur des données à caractère personnel du travailleur continuent tout au long de la relation professionnelle. Ces activités de traitement concernent habituellement toutes les informations personnelles que l'employeur a demandés et/ou obtenus de ses travailleurs.

⁸ Les autorités de contrôle suivantes ont contribué au travail de ce sous-groupe: AU, B, DE, E, EL, F, IR, IT, NL, UK.

Tous les employeurs collectent des données salariales et fiscales sur leurs travailleurs. Le traitement de ces données à caractère personnel est nécessaire à la relation professionnelle ou au respect des obligations légales, (sécurité sociale, paiement des impôts) auquel l'employeur est assujéti. Dans certains États membres, les employeurs collectent et traitent des informations médicales qu'ils stockent dans des dossiers maladie; dans d'autres, ces informations se limitent à l'absentéisme pour cause de maladie.

En effet, les employeurs évaluent les performances de leurs travailleurs en collectant des informations personnelles directement auprès des travailleurs ou par d'autres moyens, y compris le contrôle et la surveillance électroniques.

Enfin, bien que la collecte de données à caractère personnel relatives à un travailleur prenne normalement fin au terme de la relation professionnelle, l'employeur en poursuit parfois le traitement. Les employeurs conservent généralement ces données pendant un certain temps, souvent par simple souci de se conformer à l'obligation légale d'archivage pour une durée déterminée.

Exemples de dossiers professionnels impliquant généralement le traitement de données à caractère personnel couvert par la directive 95/46/CE
<i>Formulaires de candidature et références</i>
<i>Données salariales et fiscales - informations relatives aux avantages fiscaux et sociaux</i>
<i>Dossiers maladie</i>
<i>Dossiers congés annuels</i>
<i>Dossiers congés sans solde/congés exceptionnels</i>
<i>Dossiers d'évaluation/appréciation annuelle</i>
<i>Documents relatifs à une promotion, un transfert, Une formation ou des sanctions disciplinaires</i>
<i>Documents relatifs aux accidents de travail</i>
<i>Informations générées par des systèmes informatiques</i>

<i>Fiches de présence</i>
<i>Composition de famille</i> ⁹
<i>Remboursement de frais, par exemple, frais de déplacement</i>

Comme la Cour européenne des Droits de l'Homme l'a souligné dans l'affaire Niemitz c. Allemagne:

*"le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de vie privée comme excluant les activités professionnelles ou commerciales: après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur. Un fait, souligné par la Commission, le confirme: dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort."*¹⁰

⁹ Données traitées pour faciliter l'accès à certains services comme les écoles maternelles, les études, transport/voyage, etc.

¹⁰ CEDH, 23 novembre 1992, Séries A No. 251/B, § 29.

3. Principaux instruments internationaux

3.1. Communauté européenne

- ❑ Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.¹¹
- ❑ Directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.¹²
- ❑ Article 286 de la version consolidée du traité instituant la Communauté européenne.
- ❑ Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.
- ❑ Charte des droits fondamentaux de l'Union européenne¹³.

3.2. Conseil de l'Europe

- ❑ Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales (CEDH), art. 8.
- ❑ Convention du Conseil de l'Europe (108) pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel¹⁴

¹¹ JO L 281, 23.11.1995, p. 31. http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

¹² JO L 24, 30.01.98, p. 1.

http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf

¹³ http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf

Article 8. Protection des données à caractère personnel Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi.

Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
Le respect de ces règles est soumis au contrôle d'une autorité indépendante

¹⁴ <http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=>

- ❑ Recommandation du Conseil de l'Europe n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi.¹⁵
- ❑ Recommandation du Conseil de l'Europe (97) 5 relative à la protection des données médicales.¹⁶
- ❑ Recommandation du Conseil de l'Europe (86) 1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociales.¹⁷

3.3. Organisation internationale du Travail

- ❑ Le Code de pratiques de l'Organisation Internationale du Travail sur la protection des données à caractère personnel relatives aux travailleurs (1997)

4. Législations nationales relatives à la protection des données s'appliquant au contexte professionnel

a) États membres de l'Union européenne.

Autriche

- ❑ Législation générale: loi fédérale sur la protection des données à caractère personnel¹⁸
- ❑ Disposition explicite concernant l'utilisation de données sensibles sur le lieu de travail¹⁹
- ❑ Procédures d'information et de consentement avant l'introduction de mesures de contrôle sur le lieu de travail: droit du travail²⁰

¹⁵ <http://cm.coe.int/ta/rec/1989/89r2.htm>

¹⁶ <http://cm.coe.int/ta/rec/1997/97r5.html>

¹⁷ [http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R\(86\)1E.htm](http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm)

¹⁸ <http://www.bka.gv.at/datenschutz/indexe.htm>

¹⁹ Sect 9, sous-paragraphe 11

²⁰ Loi constitutionnelle sur le travail n° 22/1974, art. 96

- ❑ Interdiction spécifique pour les employeurs de faire subir aux travailleurs ou candidats des tests génétiques²¹.

Belgique

- ❑ Législation générale: loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel²²
- ❑ Réglementation spécifique concernant le traitement de données à caractère médical relatives aux examens médicaux des travailleurs
- ❑ Décret régional concernant le traitement de données sensibles dans des agences de remplacement, de recrutement et bureaux de sélection.
- ❑ Deux accords collectifs (n° 13 et 68) contenant des dispositions relatives aux procédures de consultation et d'information avec les employés.

Danemark

- ❑ Législation générale: loi sur le traitement des données à caractère personnel (loi n° 429 du 31 mai 2000)²³
- ❑ Législation spécifique relative au traitement des données à caractère médical relatives aux examens médicaux des travailleurs
- ❑ Législation spécifique pour les fonctionnaires

Finlande

- ❑ Législation générale: loi sur les données à caractère personnel (523/1999)²⁴
- ❑ Législation spécifique sur la protection de la vie privée dans la vie active (loi adoptée par le Parlement finlandais en mai 2001 devant entrer en vigueur à l'automne 2001).²⁵

²¹ Loi sur le génie génétique n° 510/1994, sect. 67

²² <http://www.privacy.fgov.be/loi98coordi.htm>

²³ <http://www.datatilsynet.dk/eng/index.html>

²⁴ <http://www.tietosuoja.fi/uploads/hopxtvf.HTM>

²⁵ Il s'agit de la première législation communautaire traitant spécifiquement de la protection des données à caractère personnel sur le lieu de travail. Cette loi aborde la plupart des problèmes mentionnés dans le présent avis de même que des aspects particuliers, tels que des tests évaluant l'adéquation des employés (section 5), des examens médicaux et autres tests (section 6), des tests génétiques (section 7), des données sur l'état de santé des employés (section 8) ou des procédures relatives à la surveillance technique et accord d'utilisation des réseaux informatiques (section 9).

France

- ❑ Législation spécifique: loi n° 78-17 du 6 janvier 1978 sur la protection de la vie privée des individus.²⁶
- ❑ Règles spécifiques relatives à la protection des données relatives aux travailleurs dans le Code du travail²⁷

Allemagne

- ❑ Législation générale: loi fédérale sur la protection des données à caractère personnel (BDSG)²⁸
- ❑ Réglementations détaillées concernant la protection des données des fonctionnaires (loi-cadre régissant le droit des fonctionnaires -BRRG- , 56 à 56 et loi fédérale relative aux fonctionnaires–BBG- 90 à 90 g. toutes deux adoptées en 1997).
- ❑ Implémentation des installations techniques qui peuvent être utilisées pour le contrôle de la performance, du comportement, uniquement avec l'accord du comité de travailleurs, conformément aux réglementations légales du droit collectif du travail (secteurs public et privé).

Grèce

- ❑ Législation générale 2472/97 sur la protection des individus relative au traitement des données à caractère personnel ²⁹

Irlande

- ❑ Législation générale: loi de 1988 sur la protection des données³⁰

²⁶ <http://www.cnil.fr/textes/index.htm>

²⁷ http://www.legifrance.gouv.fr/html/frame_codes1.htm

²⁸ http://www.bfd.bund.de/information/BDSG_neu.pdf

²⁹ <http://www.dpa.gr/2472.htm>

³⁰ <http://www.dataprivacy.ie/6ai.htm>

Italie

- ❑ Législation générale: protection des individus et autres sujets concernant le traitement des données à caractère personnel: loi n° 675 du 31 décembre 1996³¹
- ❑ Dispositions spécifiques limitant la surveillance et le contrôle des travailleurs

Luxembourg

- ❑ Législation générale sur l'utilisation des données dans les transferts électroniques (loi du 31 mars 1979)
- ❑ Nouveau projet de loi présenté en octobre 2000, première lecture prévue à l'automne 2001.

Pays-Bas

- ❑ Législation générale: loi du 6 juillet 2000³² sur la protection des données à caractère personnel (entrée en vigueur le 1 septembre 2001).
- ❑ Dispositions en droit du travail sur les procédures d'information et de consentement en accord avec les comités d'entreprise.³³
- ❑ Législation relative aux dossiers maladie et paiement des employés (janvier 2001).³⁴
- ❑ Législation concernant l'enregistrement des origines ethniques des employés (avril 1998).
- ❑ Loi d'identification (décembre 1993) et loi sur le numéro d'identification personnel (janvier 2001)³⁵

³¹ <http://astra.garanteprivacy.it/garante/frontdoor/1.1003..00.html?LANG=2>

³² http://www.registratiekamer.nl/bis/top_2_6.html

³³ Lois sur les conditions de travail (novembre 1998), art. 5.1.-5.3, loi sur les comités d'entreprise (octobre 1999), réglementations générales du travail pour le personnel gouvernemental (décembre 2000)

³⁴ Article 29. Les syndicats devraient être informés, entendus et dans certains cas, donner leur approbation lorsqu'il existe un accord collectif.

³⁵ Uniquement dans certains cas nécessaires à la satisfaction d'une obligation légale, l'employeur est autorisé à utiliser le numéro d'identification personnel.

Portugal

- ❑ Législation générale: loi 67/98 du 26 octobre 1998³⁶

Espagne

- ❑ Législation générale: loi organique 15/99 du 13 décembre sur la protection des données à caractère personnel³⁷
- ❑ Arrêté royal 994/1999 sur les mesures de sécurité obligatoires applicables aux fichiers informatiques contenant des données à caractère personnel³⁸.
- ❑ Arrêté royal 1/1995 sur le texte consolidé de la loi sur le statut des travailleurs.³⁹
- ❑ Loi organique 11/1985 sur la liberté des syndicats.
- ❑ Loi sur la prévention des accidents de travail⁴⁰ («Labour Hazard Prevention Law 31/1995).

Suède

- ❑ Législation générale: loi du 24 octobre 1998 sur les données à caractère personnel (1998:204)⁴¹
- ❑ Dispositions spécifiques concernant une consultation avec les délégués des travailleurs lors de la mise en place de caméras de surveillance. Réglementation stipulant que le contrôle des performances des travailleurs n'est pas autorisé à leur insu, ni sans avoir entendu les délégués syndicaux avant l'introduction des mécanismes de contrôle.⁴²

³⁶ <http://www.cnpd.pt/Leis/leis.htm>

³⁷ <https://www.agenciaprotecciondatos.org/datd1.htm>

³⁸ <http://www.agenciaprotecciondatos.org/datd8.htm>

³⁹ http://www.ccoo.es/legislacion/ley11_8S.htm

⁴⁰ <http://www.websindical.com/legis/prl.htm>

⁴¹ http://www.datainspektionen.se/in_english/

⁴² Article 11 Lag (1976:580), Articles 1 and 3 Lag (1998: 150)

Royaume-Uni

- ❑ Législation générale: loi de 1998 sur la protection des données⁴³

b) États membres de l'EEE

Norvège

- ❑ Législation générale: loi sur la protection des données à caractère personnel⁴⁴
- ❑ Des dispositions spécifiques de l'accord collectif principal réglementent la question du contrôle du lieu de travail, en accord avec les procédures d'information et de consultation et les délégués syndicaux.

Islande

- ❑ Loi générale: loi n° 77/2000 sur la protection des individus concernant le traitement de données à caractère personnel⁴⁵

5. Champ d'application et mise en oeuvre de la directive

La directive 95/46/CE s'applique au traitement, totalement ou partiellement automatisé, de données à caractère personnel et au traitement, autre qu'automatisé, de données à caractère personnel qui font partie intégrante d'un fichier ou qui sont destinées à en faire partie. On entend par "données à caractère personnel" toute information relative à une personne physique identifiée ou identifiable. La définition du traitement est très vaste. Par conséquent, toute collecte, utilisation ou stockage d'informations relatives aux travailleurs relayée par voie électronique tombera certainement dans le champ d'application de la directive.

⁴³ <http://wood.ccta.gov.uk/dpr/dpdoc.nsf>

⁴⁴ <http://www.datatilsynet.no/>

⁴⁵ <http://www.personuvernd.is/tolvunefnd.nsf/pages/1E685B166D04084D00256922004744AE>

La surveillance de l'accès à Internet ou au courrier électronique du travailleur s'inscrit dans le champ d'application de la directive. Le contrôle de la messagerie électronique implique nécessairement le traitement de données à caractère personnel. La surveillance de l'accès à Internet, sauf si elle se situe à un niveau si élevé que l'accès à certains sites ou modèles d'accès ne peut pas être lié à une personne en particulier, et si seules des informations agrégées sont produites, implique nécessairement le traitement de données à caractère personnel sur le travailleur y accédant. Le traitement de données sonores et visuelles dans le contexte professionnel entre dans le champ d'application de la directive et la vidéo-surveillance des travailleurs est couverte par ses dispositions.

Tous les dossiers manuels n'entrent pas nécessairement dans le champ d'application de la directive, sauf s'ils font partie d'un fichier de données à caractère personnel. Il s'agit de tout ensemble structuré de données à caractère personnel accessibles selon certains critères spécifiques, centralisé, décentralisé ou dispersé sur une base géographique ou fonctionnelle. La plupart des dossiers professionnels sont susceptibles de répondre à cette définition. Toutefois, dans certains pays, les mesures de mise en oeuvre peuvent exclure certaines notes manuscrites ne faisant pas partie d'un système d'archivage, mais étant donné leur nature nécessairement structurés, les dossiers professionnels contiendront la plupart des informations relatives aux travailleurs, que ce soit par un système centralisé ou par des responsables de secteurs.

Outre la directive générale relative à la protection et au traitement des données à caractère personnel (95/46/CE), la directive concernant le traitement des données à caractère personnel dans le secteur des télécommunications (97/66/CE) peut également s'avérer pertinente. Elle précise et complète la directive 95/46/CE relative au traitement de données à caractère personnel dans le secteur des télécommunications. Même s'il entre dans le champ d'application de la directive 95/46/CE, le contrôle des communications électroniques par les employeurs, y compris l'accès à Internet et le courrier électronique, pourrait également entrer dans le champ d'application de la directive 97/66/CE, qui est en train d'être revu dans le contexte de la révision du cadre juridique communautaire sur les télécommunications.

Le groupe de travail aimerait souligner que l'application de la loi sur la protection des données ne peut pas être dissociée de celle du droit du travail. Il existe nécessairement une interaction entre les deux. La nature précise de cette interaction varie d'un État membre à l'autre, mais généralement, il en est ainsi:

- ❑ L'utilisation croissante des technologies de l'information et des communications dans le contexte professionnel augmente le degré d'interaction, dans la mesure où les pratiques professionnelles s'appuient de plus en plus sur le traitement de données à caractère personnel auquel s'appliquent les principes généraux de protection de données;
- ❑ Tous les problèmes impliquant le traitement de données à caractère personnel dans le contexte professionnel ne relèvent pas exclusivement de la protection des données;
- ❑ L'interaction est nécessaire et précieuse. Elle devrait contribuer à l'élaboration de solutions qui protègent adéquatement les intérêts des travailleurs.

6. Légalité du traitement de données à caractère personnel

Tout traitement de données à caractère personnel, dans le contexte professionnel également, doit, pour être légal, répondre aux exigences de la section II de la directive 95/46/CE. Dans tous les cas, il est nécessaire d'établir une base légale pour ce traitement en vertu des articles 6, 7 et 8 de la directive (ce dernier porte sur des données sensibles). Le responsable du traitement doit également respecter d'autres exigences comprenant:

EXIGENCES COMPLEMENTAIRES AUX ARTICLES 6, 7 ET 8
INFORMATION DE LA PERSONNE CONCERNEE (ARTICLES 10 ET 11)
DROIT D'ACCES DE LA PERSONNE CONCERNEE AUX DONNEES (ARTICLE 12)
DROIT D'OPPOSITION DE LA PERSONNE CONCERNEE (ARTICLES 14 ET 15)
CONFIDENTIALITE ET SECURITE DES TRAITEMENTS (ARTICLES 16 ET 17)
OBLIGATION DE NOTIFICATION A L'AUTORITE DE CONTROLE (ARTICLES 18, 19, 20, 21)

La directive autorise certaines dérogations limitées à certaines des exigences ci-dessus, mais pas à l'article 7 ou 8 (articles 9 et 13).

7. Critères pour rendre le traitement de données légitime. Article 7.

Au moins un des critères spécifiés à l'article 7 doit être satisfait si des données à caractère personnel sont traitées dans le contexte professionnel. Chacun de ces critères nécessite que, dans tous les cas, le traitement en cours soit "nécessaire à" l'accomplissement de l'objectif en question plutôt que simplement utile à son accomplissement.

Les critères les plus pertinents sont:

LE TRAITEMENT EST NECESSAIRE A L'EXECUTION D'UN CONTRAT AUQUEL LA PERSONNE CONCERNEE EST PARTIE... (ARTICLE 7.1.B)

Les relations professionnelles sont très souvent fondées sur un contrat de travail entre l'employeur et le travailleur. Pour satisfaire à ses obligations contractuelles, par exemple, payer le travailleur, l'employeur doit traiter des données à caractère personnel.

LE TRAITEMENT EST NECESSAIRE AU RESPECT D'UNE OBLIGATION LEGALE... (ARTICLE 7.1.C)

La législation du travail peut imposer des obligations légales à l'employeur, qui nécessairement, doit recourir au traitement de données à caractère personnel. L'employeur peut se trouver dans l'obligation légale de communiquer certaines données à caractère personnel, par exemple, aux autorités fiscales ou de traiter des données relatives aux paiements de la sécurité sociale.

LE TRAITEMENT EST NECESSAIRE A LA REALISATION DE L'INTERET LEGITIME POURSUIVI PAR LE RESPONSABLE DU TRAITEMENT OU PAR LE OU LES TIERS AUXQUELS LES DONNEES SONT COMMUNIQUEES, A CONDITION QUE NE PREVALENT PAS L'INTERET OU LES DROITS ET LIBERTES FONDAMENTAUX DE LA PERSONNE CONCERNEE...

(Article 7.1.F).

Ce critère nécessite de trouver un équilibre entre les intérêts de l'employeur et ceux des employés. Certaines autorités de contrôle ont publié des orientations sur la manière d'atteindre un équilibre entre les intérêts du responsable du traitement et ceux de la personne concernée. Il est important de noter que si ce critère est pris en

considération, le travailleur a le droit de s'opposer au traitement sur des bases légales (article 14).

D'autres critères moins susceptibles d'être pertinents sont:

- **LE TRAITEMENT EST NECESSAIRE A LA SAUVEGARDE DE L'INTERET VITAL DE LA PERSONNE CONCERNEE.**

(article 7.1.D)

Cet article peut être pertinent dans le contexte de la protection de la sécurité.

- **LE TRAITEMENT EST NECESSAIRE A L'EXECUTION D'UNE MISSION D'INTERET PUBLIC....**

(article 7.1.E).

Les circonstances dans lesquelles ce critère est pertinent dans un contexte professionnel devraient être très limitées.

Si aucun de ces critères n'est applicable au traitement des données d'un travailleur par l'employeur, celui-ci peut recourir à la solution alternative d'obtenir le consentement du travailleur dénué de toute ambiguïté pour le traitement. Le terme "consentement" sera défini ultérieurement à la section 11.

8. Le traitement de données sensibles. Article 8.

La directive identifie des catégories particulières de données, qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement de données relatives à la santé et à la vie sexuelle. La directive accorde aussi une protection particulière aux données relatives aux infractions, condamnations criminelles ou mesures de sécurité. Les États membres n'ont pas la liberté d'allonger, ni de réduire cette liste. Bien sûr, ils

peuvent établir des garanties spéciales pour certaines catégories de données sensibles, telles que les données génétiques.

L'article 8 se base sur le principe selon lequel le traitement de données portant sur des catégories particulières ("données sensibles") est interdit. Il énumère ensuite plusieurs exceptions qui définissent plusieurs circonstances dans lesquelles cette interdiction ne s'applique pas. Les législations nationales de certains États membres peuvent limiter la mesure dans laquelle les employeurs peuvent tirer parti de ces exceptions. En conséquence, les États membres utilisent ces exceptions avec plus ou moins d'élasticité. La directive autorise les États membres à ajouter des exceptions pour des raisons substantielles d'intérêt public.

Si aucune de ces autres exceptions n'est applicable, un employeur peut se fonder sur le consentement explicite de la personne concernée pour le traitement de données sensibles, sauf si la législation de son État membre prévoit que l'interdiction de traitement des données sensibles ne peut être levée par le consentement de la personne, comme c'est le cas dans certaines conditions en Belgique. Les possibilités d'utilisation du consentement dans la relation professionnelle sont très limitées, comme l'indique la section 11.

Exemple

Les circonstances dans lesquelles le traitement de données sensibles par un employeur est limité par la législation nationale, même si elles font partie des exceptions reprises à l'article 8, sont le traitement des données relatives à l'état de santé d'un travailleur en France et les données génétiques en Autriche. Un exemple d'exceptions supplémentaires instaurées par les États membres est le traitement de données sensibles, telles que l'origine ethnique ou raciale pour assurer l'égalité du traitement. Plusieurs États membres ont élaboré des dispositions spécifiques à cet égard.

D'autres exemples encore (à reformuler). Si la législation nationale le permet et supposant que le principe de limitation soit respecté, les données sensibles les plus susceptibles d'être collectées par les employeurs dans le contexte professionnel sont les suivantes:

•	L'appartenance à un syndicat	-	par exemple, pour permettre à l'employeur de déduire du salaire les frais de souscription au profit du syndicat
•	Santé	-	par exemple, pour une indemnité maladie, conformité aux exigences de santé et de sécurité, fourniture d'un programme de médecine du travail, fourniture d'indemnités d'assurance ou de retraite
•	Infractions criminelles	-	par exemple, concernant une enquête pour fraude de la part de travailleurs, veiller à ce que les travailleurs condamnés pour malhonnêteté n'occupent pas un poste de confiance.

Les exceptions de l'article 8 sont bien plus strictes que les critères de l'article 7.

Celles qui sont les plus susceptibles d'être pertinentes dans le contexte professionnel sont les suivantes:

LE TRAITEMENT EST NECESSAIRE AUX FINS DE RESPECTER LES OBLIGATIONS ET LES DROITS SPECIFIQUES DU RESPONSABLE DU TRAITEMENT EN MATIERE DE DROIT DU TRAVAIL, DANS LA MESURE OU IL EST AUTORISE PAR UNE LEGISLATION NATIONALE PREVOYANT DES GARANTIES ADEQUATES.

(ARTICLE 8.2.B)

Le contexte professionnel est immanquablement visé et peut avoir un champ d'application plus large. Tout dépend dans quelle mesure les droits et obligations de l'employeur sont ancrés dans le droit du travail de chaque État membre ou s'il s'agit seulement de coutumes ou pratiques.

LE TRAITEMENT EST NECESSAIRE A LA CONSTATATION, A L'EXERCICE OU A LA DEFENSE D'UN DROIT EN JUSTICE.

(ARTICLE 8.2.E)

Le contexte professionnel est concerné, notamment concernant des plaintes des travailleurs à l'encontre de leur employeur, peut-être en raison d'un licenciement abusif, par exemple, transfert de données relatives au travailleur à des avocats ou à des tribunaux. Il est toutefois limité aux plaintes éventuelles et actuelles. Il ne justifierait pas le traitement de données sensibles de tous les travailleurs, parce qu'un jour l'un d'eux pourrait tenter une action en justice.

LE TRAITEMENT EST NECESSAIRE A DES FINS DE MEDECINE PREVENTIVE ET LE TRAITEMENT DE CES DONNEES EST EFFECTUE PAR UN PRATICIEN DE LA SANTE TENU AU SECRET PROFESSIONNEL OU PAR UNE AUTRE PERSONNE EGALEMENT SOUMISE A UNE OBLIGATION DE SECRET EQUIVALENTE.

(ARTICLE 8.3)

Cette exception sera pertinente dans un contexte de programmes de médecine du travail.

En outre, l'article 20 de la directive impose des garanties supplémentaires en disposant que les opérations de traitement susceptibles de présenter des risques particuliers au

regard des droits et libertés des personnes concernées doivent faire l'objet d'un contrôle préalable par les autorités de contrôle.

9. Principes relatifs à la qualité des données. Article 6.

Un responsable de traitement doit répondre aux exigences de sa législation nationale mettant en oeuvre l'article 6 de la directive et satisfaisant aux critères de l'article 7 et dans le cas de données sensibles à une exception de l'article 8. L'article 6 prévoit que les données à caractère personnel doivent être:

- (a) traitées loyalement et licitement;
- (b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités;
- (c) adéquates, pertinentes et non excessives;
- (d) exactes et, si nécessaire, mises à jour;
- (e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

Ces principes s'appliquent au traitement des données à caractère personnel dans le contexte professionnel, de même qu'ailleurs. Ils tiennent compte des circonstances dans lesquelles les données personnelles sont traitées.

Exemple :

Le fait qu'une banque détienne dans ses données le numéro de sécurité sociale de son client peut être excessif, mais si un employeur n'est pas en possession de cette information sur ses travailleurs, il ne serait pas en mesure de remplir ses obligations. Plusieurs autorités de contrôle sont d'avis que la collecte des numéros de sécurité sociales de tous les candidats à un emploi est susceptible d'être disproportionnée et ainsi d'enfreindre les exigences de protection des données. Seul le candidat retenu devrait être invité à fournir ce genre de détails.

L'exigence de traitement loyal et licite des données à caractère personnel garantit un haut niveau de protection. Pour assurer un traitement licite des données à caractère personnel, elles doivent être traitées de manière à ne pas enfreindre la loi sur la protection des données ou autres dispositions légales. Il peut s'agir de dispositions légales générales pertinentes dans le contexte professionnel, par exemple une obligation de confiance de l'employeur vis-à-vis des travailleurs ou autres dispositions légales spécifiques relatives à l'emploi, par exemple, une loi interdisant certains types de discrimination professionnelle.

Pour garantir un traitement loyal des données, elles doivent être traitées de manière à ne pas être injustes vis-à-vis des personnes concernées. Il s'agit là d'une disposition potentiellement très vaste. Par exemple, la surveillance des travailleurs, même si elle répond en tous points aux exigences de la directive, doit néanmoins être réalisée de manière à être "loyale" à l'égard des travailleurs surveillés. C'est un test de proportionnalité supplémentaire.

Il est important de rappeler que les articles 6, 7 et 8 ont un effet cumulatif. Les principes définis à l'article 6 sont un élément essentiel de la protection que la directive accorde aux travailleurs concernant le traitement de données à caractère personnel. Les données à caractère personnel en possession de l'employeur peuvent être abusives, même si elles ont été fournies spontanément par le travailleur qui a donné son accord pour leur stockage. Les législations nationales de certains États membres, peuvent, dans tous les

cas, empêcher la collecte de certaines données, même si le travailleur a exprimé son consentement.

Le traitement des données à caractère personnel dans le contexte du contrôle des travailleurs pourrait être injuste même si le travailleur a consenti au contrôle ou si un des autres critères de l'article 7 est satisfait. Le consentement peut entrer en ligne de compte pour déterminer si le traitement satisfait à l'article 6. La mesure dans laquelle il intervient varie d'un État membre à l'autre, mais le consentement ne peut jamais être le facteur déterminant.

9.1 Principes de base à retenir en matière de protection des données dans le contexte professionnel

Les travailleurs n'abandonnent pas leur droit à la vie privée, chaque matin, en franchissant le seuil de la porte de leur lieu de travail. Le droit à la vie privée n'est toutefois pas un droit absolu. Il doit être équilibré avec d'autres droits, libertés ou intérêts légitimes. Ceci s'applique également dans le contexte professionnel.

Aussi longtemps qu'ils font partie d'une organisation, les travailleurs doivent accepter un certain degré d'intrusion dans leur vie privée et doivent partager certaines informations personnelles avec leur employeur. Ce dernier a un intérêt légitime à traiter des données à caractère personnel relatives à ses travailleurs pour des raisons légales et légitimes, nécessaires au développement normal de la relation professionnelle et au bon fonctionnement de l'entreprise.

Dès lors, la question n'est pas de savoir si le traitement de données sur le lieu de travail est en soi une activité légale ou non. La véritable question consiste à déterminer les limites que la protection de données impose à ce genre d'activités ou inversement, les raisons qui peuvent justifier la collecte et, ensuite, le traitement de données à caractère personnel d'un travailleur donné.

Évidemment, il n'existe pas *a priori* de réponses absolues à ces questions. Le niveau toléré d'intrusion dans la vie privée dépendra largement de la nature de l'emploi et des circonstances spécifiques qui entourent et influencent la relation professionnelle.

Exemple :

Quelle quantité d'informations personnelles relatives à un travailleur potentiel un employeur est-il autorisé à collecter?

La réponse à cette question sera très différente pour un chef de la sécurité à la Banque européenne d'investissement ou pour un employé à la cafétéria dans le même établissement.

Le groupe de travail souhaiterait identifier certains principes extraits de la directive 95/46/CE, qui doivent régir toutes les activités de traitement de données dans le contexte professionnel. Les autorités de contrôle des États membres sont invitées à jouer un rôle fondamental dans l'application pratique de ces principes généraux, tenant strictement compte des spécificités des législations nationales.

PRINCIPES DE BASE EN MATIERE DE PROTECTION DES DONNEES REGISSANT LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL DES TRAVAILLEURS
FINALITE
TRANSPARENCE
LEGALITE
LE TEST DE PROPORTIONNALITE

STOCKAGE APPROPRIE DES DONNEES
SECURITE
SENSIBILISATION DU PERSONNEL

FINALITE

Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Le groupe de travail se consacre actuellement à l'élaboration d'orientations à cet égard.

Exemple :

Les adresses personnelles des travailleurs, nécessaires à des fins salariales, ne peuvent pas être utilisées ou traitées à des fins directes de marketing. Cependant, le traitement ultérieur de ces données serait autorisé pour inclure ou réévaluer les frais de déplacement dans le salaire.

TRANSPARENCE

Le principe de transparence doit toujours être pris en considération. Dans les États membres, de nombreuses opérations de traitement réalisées dans le contexte professionnel enfreignent les règles de protection de données, pas uniquement parce que le traitement est illicite *per se*, mais parce que les travailleurs n'ont pas été correctement informés à ce sujet. Les travailleurs doivent à tout le moins savoir quelles données les employeurs collectent à leur égard (directement ou à partir d'autres sources). Ils doivent

également connaître les objectifs des opérations de traitement envisagées ou menées actuellement ou à l'avenir.

La transparence est également assurée en permettant à la personne concernée d'accéder aux données la concernant.

Exemple :

Un employeur pourrait avoir un intérêt légitime à contrôler les performances de ses employés en évaluant leurs prestations à l'aide d'ordinateurs (par exemple, surveiller le temps qu'un employé a passé à dactylographier, le nombre de fichiers enregistrés, l'heure à laquelle il a allumé et éteint son ordinateur, etc.) Rien n'interdit ce traitement, pour autant que les travailleurs en aient été informés. Si cette surveillance a été réalisée à l'insu du personnel, le traitement des données des travailleurs est en contradiction avec les dispositions de la directive 95/46/CE.

LEGITIMITE

Toute opération de traitement, même totalement transparente vis-à-vis des travailleurs, ne peut avoir lieu que si elle est légitime. Bien que nous ayons analysé cette question plus en profondeur, il est toutefois important de clarifier d'emblée que l'article 7, point f) de la directive⁴⁶ ne laisse pas carte blanche à l'employeur pour tout type de traitement des données relatives aux travailleurs. Le traitement ne doit pas seulement réussir les deux tests de proportionnalité et de nécessité mentionnés ci-après, il doit aussi ne pas porter préjudice, de manière injustifiée, aux droits et libertés des personnes concernées.

Exemple :

Un employeur a un intérêt légitime à évaluer les performances de ses travailleurs et, pour ce faire, il devra souvent recourir au traitement de données à caractère personnel. Ce critère ne sera satisfait que si le contrôle des performances ne porte pas préjudice, de manière injustifiée, aux droits et libertés des personnes concernées. La section 12 traite de la manière dont il peut le faire, par exemple à l'aide d'un certain type de surveillance d'accès à Internet ou au courrier électronique.

LE TEST DE PROPORTIONNALITE

Enfin, supposant que les travailleurs en ont été informés et que le traitement est légitime, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement⁴⁷.

⁴⁶ L'article dispose que: *Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, en l'occurrence, l'employeur.*

⁴⁷ Article 6.1.c) de la directive 95/46/CE

Supposant que les travailleurs ont été informés de l'opération de traitement et présumant que ce traitement est légitime et proportionné, le traitement doit toujours être juste avec le travailleur⁴⁸.

Cette exigence de proportionnalité potentiellement vaste présente plusieurs aspects dans le contexte professionnel. Toutefois, son principal effet est que les employeurs devraient toujours traiter les données à caractère personnel de la façon la moins intrusive possible.

Plusieurs éléments sont à prendre en considération en vue d'assurer cette discrétion: les risques en cause, le nombre de données impliquées, la finalité du traitement, etc.

Exemple:

Les employeurs peuvent souhaiter savoir (pour certains emplois) si les candidats possèdent une voiture et ont le permis de conduire. L'employeur potentiel est en droit de demander ces informations, mais il serait contraire à ce principe de demander le modèle ou la couleur de la voiture en question.

⁴⁸ Article 6: *Les États membres prévoient que les données à caractère personnel doivent être traitées loyalement et licitement.*

EXACTITUDE ET CONSERVATION DES DONNEES

Les dossiers professionnels des employeurs doivent être exacts et au besoin mis à jour. L'employeur doit prendre toutes les mesures raisonnables pour que les données inexacts ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées. Les dossiers professionnels doivent être conservés sous une forme qui ne permette l'identification des travailleurs que pour la durée nécessaire à la réalisation des objectifs pour lesquels elles ont été collectées ou pour lesquels elles sont traitées ultérieurement.

Exemple:

L'évaluation annuelle d'un travailleur contient des données relatives à une date concrète et un contact donné. Après plusieurs années, il n'est en principe plus nécessaire de stocker les données relatives à ces évaluations. C'est pourquoi le délai de conservation devrait être limité à deux ou trois ans au maximum après l'évaluation.

Les employeurs peuvent s'assurer de l'exactitude des données personnelles des travailleurs, par exemple, en leur communiquant une édition annuelle de leur dossier professionnel.

SECURITE

L'employeur doit mettre en oeuvre des mesures techniques et organisationnelles appropriées sur le lieu de travail pour garantir la sécurité des données à caractère personnel relatives à ses travailleurs. Une protection particulière doit être accordée quant à un accès ou une diffusion non autorisée. Les données à caractère personnel doivent être mises à l'abri de la curiosité des autres travailleurs et de tiers. La technologie actuelle offre des moyens raisonnables empêchant un accès ou une diffusion non autorisée, et permettant dans tous les cas l'identification du membre du personnel accédant aux fichiers.

Mesures de sécurité de base sur le lieu de travail:

- ❑ **Systèmes d'identification/mot de passe permettant d'accéder aux dossiers professionnels informatisés.**
- ❑ **Ouverture de session et suivi de l'accès et diffusion**
- ❑ **Copies de sauvegarde**
- ❑ **Cryptage des messages, en particulier si les données sont transférées à l'extérieur de l'organisation.**

SENSIBILISATION DU PERSONNEL

Le personnel chargé du traitement des données à caractère personnel d'autres travailleurs ou ayant des responsabilités dans ce domaine, doit être informé de la protection des données et recevoir une formation appropriée. Les membres du personnel doivent être sensibilisés aux conséquences possibles d'un traitement illicite, pour eux, pour l'organisation et évidemment, pour la vie privée de leurs collègues. Sans une formation appropriée du personnel chargé du traitement des données à caractère personnel, le respect de la vie privée des travailleurs sur leur lieu de travail ne pourra jamais être correctement assuré.

10. Consentement

Il doit ressortir clairement de ce qui précède que le traitement de données à caractère personnel dans le contexte professionnel, surtout s'il ne concerne pas de données sensibles, ne nécessite pas, dans de nombreux cas, le consentement du travailleur. Le consentement devrait être une solution alternative, si les critères de l'article 7 ou les exceptions de l'article 8 sont applicables. Même lorsque le consentement s'applique, il doit être valable et l'employeur doit toujours répondre à d'autres exigences de la directive dont l'article 6 et l'article 15 relatif aux décisions automatisées. En outre, le travailleur doit avoir été informé du traitement, comme le prévoient les articles 10 et 11.

La directive définit le consentement comme: "toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à

caractère personnel la concernant fassent l'objet d'un traitement." S'il s'agit de données sensibles, le consentement doit en outre être explicite. Le groupe de travail "article 29" est d'avis que si le consentement du travailleur est nécessaire et que l'absence de consentement peut entraîner un préjudice réel ou potentiel pour le travailleur, le consentement n'est pas valable au titre de l'article 7 ou de l'article 8, dans la mesure où il n'est pas donné librement. Si le travailleur n'a pas la possibilité de refuser, il ne s'agit pas de consentement. Le consentement doit toujours être donné librement. En conséquence, le travailleur doit avoir la possibilité de se dégager de son consentement sans préjudice.

Un pierre d'achoppement peut exister si le consentement est une condition d'emploi. Le travailleur peut, en théorie, refuser de donner son consentement, mais il peut perdre alors une opportunité d'emploi. Dans ces circonstances, le consentement n'étant pas donné librement, n'est donc pas valable. La situation est encore plus claire, comme c'est souvent le cas, lorsque tous les employeurs imposent des conditions d'emploi identiques ou similaires.

LE GROUPE DE TRAVAIL "ARTICLE 29" EST D'AVIS QUE SI UN EMPLOYEUR DOIT TRAITER DES DONNEES A CARACTERE PERSONNEL COMME CONSEQUENCE INEVITABLE ET NECESSAIRE DE LA RELATION PROFESSIONNELLE, IL FAIT FAUSSE ROUTE S'IL ESSAIE DE LEGITIMER CE TRAITEMENT PAR LE CONSENTEMENT. L'ON PEUT RECOURIR AU CONSENTEMENT S'IL S'APPLIQUE STRICTEMENT AU CAS OU LE TRAVAILLEUR EST COMPLETEMENT LIBRE DE LE DONNER ET A LA POSSIBILITE D'Y RENONCER PAR LA SUITE SANS PREJUDICE.

Dans les autres cas, le travailleur doit également recevoir clairement des informations (article 10) et les critères des articles 7 et 8 devront être suffisamment étendus pour légitimer le traitement sur d'autres bases que le consentement.

Le groupe de travail est conscient que la législation de plusieurs États membres a conféré aux délégués de travailleurs locaux le rôle de contribuer à la protection des droits des travailleurs en matière de protection de données. Par exemple, dans certains États

membres, les sociétés doivent recevoir l'accord des comités d'entreprise avant d'introduire des contrôles sur le lieu de travail.

11. Droits individuels concernant la protection des données.

Les travailleurs, sujets de la collecte de données, jouissent des droits accordés par la directive 95/46/CE.

Le plus important de ces droits est le droit d'accès, prévu à l'article 12 de la directive, disposant que toute personne concernée a le droit d'obtenir du responsable du traitement (en l'occurrence l'employeur):

a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs:

- la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,
- la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,
- la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

Les personnes concernées ont aussi le droit de s'opposer, pour des raisons prépondérantes et légitimes tenant à leur situation particulière, à ce que l'employeur traite les données les concernant, même si la législation nationale en dispose autrement (article 14 de la

directive) et ont le droit d'obtenir réparation du préjudice subi à la suite d'un traitement illégal ou de toute autre opération contraire à la législation relative à la protection des données.

Le groupe de travail a déjà présenté une recommandation sur des données d'évaluation des employés⁴⁹ et pourrait préparer davantage d'orientations à l'avenir.

12. Surveillance et contrôle

Plusieurs aspects de l'application des directives 95/46/CE et 97/66/CE relatifs à la surveillance et au contrôle des travailleurs ont déjà été abordés. Le fait que les dispositions relatives à la protection de données s'appliquent au contrôle et à la surveillance des travailleurs en termes d'utilisation de courrier électronique, d'accès à Internet, de caméras vidéo ou de données de localisation ne devrait plus faire aucun doute.

L'application de la directive au contrôle et à la surveillance et l'importance accordée au sujet sont mis en évidence par des évolutions dans les États membres, tels que les rapports et initiatives mentionnés dans l'introduction.

Il convient également de noter que:

- **tout contrôle**, s'il est réalisé sur la base de l'article 7 point f) de la directive 95/46/CE et satisfait en tous points à l'article 6, **doit être une réponse proportionnée** de l'employeur aux risques qu'il encourt de porter atteinte à la vie privée légitime et autres intérêts des travailleurs.

Toute donnée à caractère personnel, détenue ou utilisée au cours du contrôle doit être **adéquate, pertinente et non excessive au regard des finalités pour lesquelles elle justifie le contrôle**. Le contrôle doit être le moins intrusif possible. Il doit cibler la zone à risques. Par exemple, les employeurs pourraient être autorisés à contrôler les données de trafic, mais certainement pas accéder au contenu des communications électroniques de leurs employés; outre les règles concernant la protection des données, les

⁴⁹ Voir recommandation 1/2000 on « Employee Evaluation Data », adoptée par le Groupe le 22 mars (WP 42, 5008/01)

communications électroniques sont protégées par des principes constitutionnels sur la confidentialité de la correspondance⁵⁰ qui ne pourraient être levés que dans des circonstances vraiment exceptionnelles qui ne sont pas (*voir version en anglais !!!*) laissées à l'appréciation de l'employeur (en règle générale, une décision judiciaire sera nécessaire).

Le contrôle, y compris la vidéo-surveillance, **doit être conforme aux exigences de transparence de l'article 10**. Les travailleurs doivent avoir connaissance de la surveillance, des finalités pour lesquelles les données sont traitées et toute autre information nécessaire à la garantie d'un traitement loyal. La directive ne traite pas de manière moins stricte le contrôle de l'utilisation d'Internet ou du courrier électronique par un travailleur si la surveillance se fait par caméra vidéo installée dans le bureau.

Exemple :

Les **données de localisation** sont un exemple spécifique dont les travailleurs pourraient ne pas avoir connaissance. Il est vrai que la protection de données de localisation sera incluse dans la proposition de directive relative au traitement de données à caractère personnel et protection de la vie privée dans le secteur des télécommunications. Cette directive devrait remplacer la directive 97/66/CE. Bien que la localisation de données sera explicitement traitée dans la nouvelle directive, ces données **entrent néanmoins dans le champ d'application des deux directives, 95/46/CE et 97/66/CE**. Les exigences de proportionnalité mentionnées dans le paragraphe précédent s'appliquent intégralement au traitement, par l'employeur, de données de localisations relatives aux travailleurs.

Le groupe de travail "article 29" reconnaît la nécessité **d'orientations supplémentaires sur l'application de la directive en matière de surveillance et de contrôle des communications électroniques des travailleurs (par exemple le courrier électronique, Internet)**. L'élaboration de ces orientations étant un véritable défi, le

⁵⁰ Voir également à l'article 7 de la Charte des droits fondamentaux de l'Union européenne, signée et proclamée à Nice le 7 décembre 2000.

groupe de travail a néanmoins demandé au sous-groupe qui a élaboré cet avis préliminaire d'entamer cette tâche.

13. Transfert de données relatives aux travailleurs vers des pays tiers

L'article 25 de la directive établit que les **données à caractère personnel ne peuvent être transférées vers des pays tiers** non communautaires **que** si le pays tiers en question garantit **un niveau de protection adéquat**.

Il convient de rappeler que quelle que soit la base du transfert reprise aux articles 25 et 26 le traitement impliqué dans le transfert doit toujours satisfaire aux articles 6 à 8 et à toutes les autres dispositions de la directive.

L'article 26 accorde des **dérogations**, lorsque:

- la personne concernée a donné son accord sans aucune ambiguïté au transfert proposé (les considérations du chapitre 10 restent applicables ici).
- le transfert est nécessaire à la réalisation d'un contrat entre la personne concernée et le responsable du traitement
- le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice
- le transfert est réalisé sur la base de solutions contractuelles, comme autorisé par un État membre et assurant des garanties adaptées.
- Le transfert est exécuté sur la base de clauses contractuelles standard approuvées par la Commission pour autant qu'il présente des garanties adaptées.

Le groupe de travail est d'avis qu'il est préférable de se fier à une protection adéquate dans le pays destinataire, plutôt que de se fier aux dérogations prévues par l'article 26, par exemple le consentement du travailleur. Si on se fie sur le consentement, celui-ci doit être exempt d'équivoque et donné librement. Les employeurs seraient mal conseillés de se fier uniquement au consentement, à l'exception de cas où, si le consentement est retiré par la suite, cela ne causera pas de problèmes.

Si le pays tiers ne garantit pas un degré de protection approprié et qu'aucune des dérogations n'est applicable, l'employeur peut également obtenir le consentement du travailleur, dénué de toute ambiguïté.

Le groupe de travail "article 29" reconnaît l'importance de ces dispositions dans le contexte professionnel. Il est clair qu'une proportion significative de transferts internationaux implique le traitement de données relatives aux travailleurs par des multinationales ou des groupes d'entreprises. Il faut garder à l'esprit que de nombreux transferts partent d'un responsable du traitement de l'UE vers un responsable du traitement extérieur. Dans ce cas, l'employeur communautaire reste un responsable du traitement tenu de répondre à une demande du travailleur d'accéder à ses données et de respecter ses autres droits.

Le groupe de travail "article 29" a accordé une grande attention au sujet des transferts internationaux. Il a publié plusieurs avis à ce sujet⁵¹.

13.1. Transfert de données relatives à l'emploi selon le système Safe Harbor

Le système américain Safe Harbor⁵² contient des dispositions spécifiques relatives au transfert et par la suite au traitement de données relatives à des travailleurs européens par des organisations américaines établies aux États-Unis.⁵³

⁵¹ Voir avis n°5/99 sur le niveau de protection de données à caractère personnel en Suisse (WP 22, 5054/99, adopté le 7 juin 1999) et avis n°6/99 concernant le niveau de protection de données à caractère personnel en Hongrie (WP 24, 5071/99, adopté le 7 septembre 1999) et le document de travail: transferts des données à caractère personnel vers des pays tiers: application des articles 25 et 26 de la directive de l'UE sur la protection des données à caractère personnel (WP 12, 5025/98, adoptée le 24 juillet 1998).

⁵² Safe Harbor JO L215 du 25 août 2000

L'on n'examinera pas en détail ces dispositions. Il peut toutefois s'avérer utile de noter que les informations professionnelles ont bénéficié d'une protection renforcée dans ce système. Par exemple, il est reconnu que *"certaines conditions applicables de manière générale au transfert à partir de quelques États membres peuvent exclure d'autres utilisations de ces informations, même après leur transfert en dehors du territoire de l'Union européenne, et que ces conditions doivent être respectées."*

En outre, les autorités européennes de contrôle demeurent compétentes pour les infractions à la protection des données professionnelles. En adhérant au système Safe Harbor, les organisations américaines s'engagent à coopérer en investiguant et en se conformant à l'avis des autorités communautaires compétentes en la matière.

13.2. Transfert des données professionnelles en vertu des clauses contractuelles standard

Les transferts de données relatives aux travailleurs sont possibles au titre de la décision de la Commission définissant des clauses standard lorsque le destinataire fait office de responsable du traitement et les incorporent dans un contrat conclu avec l'exportateur de données établi dans la Communauté.⁵⁴

Les clauses contractuelles habituelles approuvées par la Commission offrent un mécanisme alternatif pour le transfert de données à caractère personnel relatives aux travailleurs vers des filiales ou sociétés apparentées établies dans des pays tiers dont le niveau de protection des données n'est pas adéquat. En vertu des clauses contractuelles standard, toutes les catégories de données utilisées dans le contexte professionnel, même celles de nature sensibles peuvent être transférées. Les garanties établies par le contrat sont exécutoires par les travailleurs vis-à-vis de leur employeur ou vis-à-vis du responsable du traitement établi dans un pays tiers.⁵⁵

⁵³ Voir FAQ 9 "Données sur les ressources humaines"

⁵⁴ Voir décision de la Commission du 15 juin 2001 sur les clauses relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE ; JO L 181, 04.07.01; où nécessairement d'autres formalités devront être respectées au niveau national

⁵⁵ [http:// europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm](http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm)

14. Conclusions

La directive 95/46/CE s'applique intégralement et pleinement aux données à caractère personnel relatives aux travailleurs. Bien que la directive laisse à chaque État membre une certaine marge de manœuvre pour particulariser les conditions de traitement, l'application des principes contenus dans le présent avis est commune et généralement reconnue. Le présent avis a pour objectif de contribuer à une application uniforme des mesures nationales adoptées dans la directive 95/46/CE.

Il existe une interaction nécessaire et souhaitable, entre la législation sur la protection des données et les pratiques du travail. Tous les problèmes impliquant le traitement de données à caractère personnel ne sont pas exclusivement liés à la protection des données, mais cette interaction est nécessaire pour garantir des solutions qui protègent adéquatement les intérêts des travailleurs.

Les intérêts légitimes de l'employeur justifient certaines limitations à la vie privée des employés sur leur lieu de travail. Parfois, ce sont les droits ou les intérêts d'autrui qui imposent ces limitations. Toutefois, aucun intérêt commercial ne peut jamais l'emporter sur les principes de transparence, le traitement licite, la légitimation, la proportionnalité, la nécessité et autres principes énoncés dans la directive 95/46/CE. Les travailleurs peuvent toujours s'opposer au traitement lorsqu'il est susceptible d'outrepasser de manière injustifiée leurs droits et libertés fondamentales.

Étant donné la spécificité de la relation professionnelle, le consentement ne sera en principe pas un moyen de légitimer le traitement dans le contexte professionnel. Lorsqu'on y recourt, le consentement doit toujours être donné librement, de manière particulière et informée.

Le groupe de travail envisage de donner des orientations sur la surveillance et le contrôle sur le lieu de travail, mais tous les principes décrits dans le présent avis s'appliquent pleinement à ces activités.

Fait à Bruxelles, le 13 septembre 2001

Par le groupe de travail

Le président

Stefano RODOTA