11639/02/FR
WP 74

Document de travail: Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données

Adopté le 3 juin 2003

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

ÉTABLI PAR LA DIRECTIVE 95/46/CE DU PARLEMENT EUROPEEN ET DU CONSEIL DU 24 OCTOBRE 1995[1],

vu l'article29 et l'article30, paragraphes 1 (a) et 3 de ladite directive,

vu son règlement intérieur, notamment les articles12 et 14,

A ADOPTÉ LE PRÉSENT DOCUMENT DE TRAVAIL:

[1] Journal Officiel n° L 281 du 23/11/1995, p. 31, disponible au site :

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

TABLE DES MATIÈRES

Document de travail concernant des règles d'entreprise contraignantes applicables aux transferts internationaux de données

1. INTRODUCTION

Les autorités de protection des données reçoivent des demandes de transfert de données personnelles vers des pays tiers au sens de l'article 26 (2) de la directive[2]. En règle générale, ces demandes faisaient appel à des solutions contractuelles envisagées par les autorités nationales à la lumière des principes édictés dans le document de travail n° 12[3] du groupe, d'autres documents élaborés par ce dernier et particulièrement les décisions de la Commission sur les clauses contractuelles types.

Le recours aux solutions contractuelles n'est pas nouveau pour les sociétés multinationales; cependant, certains États membres étudient actuellement la possibilité de généraliser ce recours. Ces expériences doivent être sérieusement prises en considération si l'on veut évaluer les développements éventuels de la réglementation en la matière.

Parallèlement, en raison de leur ramification internationale complexe, certaines sociétés multinationales souhaiteraient avoir la possibilité d'adopter des «codes de conduite relatifs aux transferts internationaux»[4]. Ceux-ci permettraient d'encadrer le transfert international de données personnelles au sein d'un même groupe multinational, sous réserve de l'autorisation des autorités de protection des données concernées, conformément à l'article 26 (2) de la directive. Selon ces sociétés multinationales, la piste d'engagements unilatéraux, assortis de solides garanties, devrait également être exploitée.

Tant que ces engagement unilatéraux impliquent de véritables effets contraignants sur le plan juridique - notamment en ce qui concerne la protection efficace des personnes concernées après le transfert de leurs données ainsi que l'éventuelle intervention des autorités nationales de contrôle ou d'autres instances, comme cela est expliqué plus en détail dans les chapitres 3 et 5 ci-dessous -, il n'y a aucune raison d'exclure cette

---

2 Les références aux autorités de protection des données comprennent les autorités de l'Union Européenne et de l'Espace Economique Européen.

3 Document de travail: Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données, approuvé le 24 juillet 1998.

4 L'adoption de codes de conduite par les groupes est relativement fréquente. En règle générale, les multinationales adoptent des codes de conduite pour répondre notamment aux problèmes suivants: (a) gestion et conservation de livres comptables et de dossiers exacts; (b) véracité et exactitude des communications au public et aux autorités; (c) procédures telles que «*Chinese walls*» destinées à garantir que les conseils aux clients et les décisions commerciales ne fassent pas l'objet de conflits d'intérêts; (d) protection des informations confidentielles; (e) interdiction d'abus de biens sociaux; (f) lutte contre la discrimination abusive et le harcèlement; (g) interdiction de pots-de-vin et de ristournes; (h) application de pratiques commerciales déontologiques et respect des règles de concurrence sur le marché; (i) interdiction d'opérations d'initié.

possibilité. L'article 26 (2) de la directive 95/46/CE offre aux États membres une grande marge de manœuvre à cet égard.

Ceci dit, il est important de souligner qu'en vertu de la législation nationale de certains États membres, les engagements unilatéraux n'engendrent pas d'obligations ni de droits juridiquement contraignants. C'est pourquoi le groupe de travail tient à mettre en évidence le caractère général du présent document de manière à éviter tout risque d'interférence avec les législations nationales applicables, ainsi qu'il se réserve le droit de présenter d'autres solutions susceptibles d'uniformiser davantage l'utilisation des règles d'entreprise contraignantes dans l'ensemble des États membres.

Les règles d'entreprise contraignantes ne doivent pas être considérées comme la panacée dans le cadre des transferts internationaux, mais uniquement comme un instrument supplémentaire à utiliser là où les instruments existants (à savoir les décisions de la Commission en matière de clauses contractuelles types ou les principes de la «sphère de sécurité», le cas échéant) semblent particulièrement poser problème. Le présent document ne vise en aucune façon à forcer ni même simplement à inciter les États membres à utiliser un instrument en particulier pour répondre aux requêtes émanant de sociétés multinationales. Les autorités nationales de contrôle, comme tout autre organisme compétent d'ailleurs, sont totalement libres d'analyser les propositions qui leur sont présentées et d'y répondre de la manière la mieux adaptée à leur législation nationale et aux spécificités de la demande.

Le groupe de travail estime toutefois opportun d'approfondir cette réflexion au niveau de la Communauté et de s'accorder sur une série de principes et de procédures à même de faciliter le travail des sociétés et des autorités dans les États membres tout en assurant une cohérence au sein de l'Union européenne. Quoi qu'il en soit, le présent document de travail vise à contribuer à une application et à une interprétation plus harmonisées de l'article 26 (2) de la directive dans l'ensemble des États membres et à faciliter les flux de données dans les cas où le niveau de protection offert est adéquat. [5]

Enfin, le groupe de travail «Article 29» souhaite rappeler une fois de plus que l'offre de garanties suffisantes, comme le prévoit l'article 26 (2), est un vaste concept qui couvre certes les solutions contractuelles ainsi que les règles d'entreprise contraignantes mais également d'autres situations, non abordées dans le présent document, que les autorités chargées de la protection des données peuvent juger pertinentes en vue de l'octroi d'autorisations. Quoi qu'il en soit, le présent document de travail n'aborde que l'application de l'article 26 (2) de la directive dans le cas particulier des règles d'entreprise contraignantes.

Le groupe de travail «Article 29» partage également l'inquiétude de certaines autorités nationales de protection des données qui craignent, par manque de ressources, de ne pas pouvoir traiter de manière posée et négociable les nombreuses demandes d'autorisation. Il ne doute pas que les sociétés en auront conscience et qu'elles s'efforceront de soumettre leurs demandes en respectant le plus possible les recommandations contenues dans le présent document de travail.

2. LES POTENTIALITÉS DES SOLUTIONS CONTRACTUELLES

Le groupe de travail «Article 29» souhaite insister sur le fait que bien que le présent document de travail ait pour principal objet d'examiner les règles d'entreprise contraignantes (ou les codes de conduite, pour parler de manière plus conventionnelle), il ne faut pas en déduire que les solutions contractuelles sont dépassées. Au contraire, dans la foulée des décisions de la Commission relatives aux clauses contractuelles types et grâce à la précieuse aide de ce groupe de travail et des autorités nationales chargées de la protection des données, les sociétés utilisent largement ces instruments, de manière à la fois positive et encourageante (par exemple les clauses contractuelles types avec de nombreuses parties au contrat).

Le groupe de travail «Article 29» estime que le potentiel des clauses contractuelles types commence seulement à être exploité par les opérateurs. Il convient de soulever deux points à ce propos.

Premièrement, les décisions de la Commission relatives aux clauses contractuelles types ne permettent pas à un État membre de décider qu'un exportateur de données disposé à conclure un contrat dans le respect des clauses contractuelles types n'offre pas de garanties suffisantes afin que le transfert puisse s'opérer, sauf dans les circonstances particulières spécifiées dans les décisions de la Commission. En d'autres termes, les clauses contractuelles types constituent un instrument utile, pratique - actuellement à la disposition des opérateurs -, reconnu sur un plan juridique et adopté aux niveaux européen et national; un instrument qui offre aux opérateurs et aux personnes concernées un degré de garantie suffisant et identique. Dans le même temps, les États membres sont libres d'envisager le recours à d'autres arrangements contractuels pour autant qu'ils garantissent un niveau de protection suffisant des données personnelles concernées.

Deuxièmement, il est également possible, dans le contexte de l'utilisation des clauses contractuelles types, d'envisager l'application de règles d'entreprise contraignantes dans le but de permettre, sous certaines conditions[6], des transferts ultérieurs vers des destinataires autres que l'importateur de données, sans qu'il y ait besoin de conclure d'autres contrats avec ces destinataires ultérieurs. Il s'agit là d'une troisième voie intéressante à envisager entre les solutions contractuelles et le recours aux règles d'entreprise contraignantes, susceptible d'éviter les obstacles posés par l'absence de nature contraignante des engagements unilatéraux dans certains États membres. Dès lors, la circulation de données personnelles parmi les filiales d'un groupe pourrait être autorisée dans le cadre de cette solution, à condition que les garanties requises soient mises en œuvre.

[6] Par exemple en identifiant dans le contrat les destinataires supplémentaires et en annexant les règles d'entreprise contraignantes au contrat, dont elles font quand même partie intégrante, avec tous les effets juridiques que cela peut comporter.

3. DÉFINITION ET CONSIDÉRATIONS JURIDIQUES

3.1. Portée de l'instrument et définitions

L'octroi d'autorisations telles que visées à l'article 26 (2) doit faire l'objet d'une évaluation préalable des garanties mises en oeuvre par le responsable du traitement afin d'assurer un niveau de protection adéquat des données personnelles devant être transférées vers un pays tiers.

Le concept diffère donc ici de l'approbation de codes de conduite dont parle l'article 27 de la directive, qui sont définis comme des règles professionnelles visant l'application pratique des dispositions nationales en matière de protection des données dans un secteur spécifique. Dans les deux cas, les règles internes d'un groupe ne peuvent se substituer aux obligations en matière de protection des données qui lient juridiquement les filiales du groupe. Le respect de la législation nationale en vigueur constitue évidemment une condition *sine qua non* à l'octroi d'une autorisation quelle qu'elle soit.

Tout transfert vers un pays tiers consiste en la communication de données à un autre responsable du traitement des données ou sous-traitant dans un pays tiers dont la légitimité est déterminée en fonction des circonstances générales du cas, au regard des principes visés dans la directive (articles 6, 7, 8, 17 etc.). Lorsque le traitement s'effectue dans le cadre des activités d'un établissement rattaché à une filiale d'un groupe sur le territoire communautaire ou lorsque le traitement est effectué par une filiale du groupe non établie sur le territoire communautaire mais qui utilise des équipements situés sur le territoire communautaire, la directive et les dispositions nationales en vigueur s'appliquent.

Les principes de protection contenus dans les règles d'entreprise contraignantes doivent respecter les principes de protection visés dans la directive 95/46/CE. Vue sous cet angle, la mise en œuvre de règles d'entreprise contraignantes au sein de la Communauté ne pose en principe aucun problème à condition que ces règles soient conformes à la législation nationale en matière de protection des données. Si ces conditions étaient remplies, les groupes auraient la possibilité de se doter d'une politique vraiment globale en matière de protection de la vie privée.

Dans le même ordre d'idées et par définition, les règles d'entreprise contraignantes présentent un caractère global et ne doivent par conséquent pas faire l'objet d'une distinction quant à leur application. Les règles s'appliquent uniformément à l'ensemble du groupe, indépendamment du lieu d'implantation de ses filiales ou de la nationalité des personnes dont les données personnelles sont traitées, ou de tout autre critère ou toute autre considération. Toutefois, si les règles doivent toujours rester identiques et si le groupe doit s'efforcer de les respecter telles quelles, leur caractère exécutoire vis-à-vis du groupe en question peut entraîner une distinction légitime entre des données provenant de l'UE, à savoir des données personnelles jadis soumises à la législation européenne et ultérieurement transférées vers l'étranger, et d'autres catégories de données.

Pour cette dernière catégorie de données, le groupe n'est pas tenu de permettre aux personnes concernées de revendiquer ni de faire valoir l'un ou l'autre droit sur le territoire communautaire. Bien que l'inclusion d'une telle clause ne puisse constituer une condition *sine qua non* à l'octroi d'une autorisation, elle serait toutefois toujours accueillie favorablement dans la mesure où elle témoigne de l'engagement du groupe vis-à-vis de ses obligations au regard de la protection des données.

En conséquence, dans la mesure où la finalité de ces règles diffère de celle des codes de conduite visés à l'article 27 de la directive, au lieu de reprendre le terme de «codes de conduite» (ce qui pourrait prêter à confusion), il semble plus judicieux de trouver une terminologie mieux adaptée à la nature réelle de ces règles, à savoir l'offre de garanties suffisantes aux fins de la protection de données personnelles transférées en dehors de la Communauté.

Ces instruments pourraient éventuellement être repris sous la formulation **«règles d'entreprise contraignantes applicables aux transferts internationaux de données»** ou **«règles d'entreprise juridiquement exécutoires applicables aux transferts internationaux de données»**.

a) **contraignantes ou juridiquement exécutoires** car seules les clauses présentant ce caractère peuvent être perçues comme des «garanties suffisantes» au sens de l'article 26 (2);

b) **d'entreprise** dans la mesure où il s'agit de règles en vigueur au sein de sociétés multinationales, généralement élaborées sous la responsabilité du siège. Aux fins du présent document, on entend par groupe tout groupe d'entreprises liées par les règles, tel que prévu au point 3.3;

c) **applicables aux transferts internationaux de données**, car il s'agit là de la raison d'être de ces règles.

La notion de «groupe» peut varier d'un pays à l'autre et renvoyer à des réalités commerciales très différentes: il peut s'agir de sociétés multinationales étroitement liées et extrêmement hiérarchisées ou alors de groupes de conglomérats sans forte cohésion entre eux; de groupes de sociétés développant des activités économiques, et donc des opérations de traitement, fortement similaires ou encore de partenariats entre sociétés plus globaux dont les activités économiques et les opérations de traitement sont très différentes. Manifestement, ces différences structurelles et opérationnelles influent sur l'applicabilité, le modèle et la portée des règles d'entreprise contraignantes, un élément que les groupes doivent garder à l'esprit en soumettant leurs propositions.

Pour les conglomérats reposant sur une coopération moins étroite, les règles d'entreprise contraignantes ne devraient pas constituer un outil adéquat. La diversité qui caractérise ses membres et la portée plus large des activités de traitement concernées rendraient très difficile (pour ne pas dire impossible) le respect des exigences visées dans le présent document. Pour ce type de conglomérats, il serait nécessaire de distinguer des sous-groupes à l'intérieur d'un même groupe, de poser des limites et des conditions strictes aux échanges d'informations et de préciser les règles. En d'autres termes, si un instrument devait finalement s'avérer acceptable au sens de l'article 26 (2) de la directive, celui-ci serait certainement très différent des règles d'entreprise contraignantes analysées dans le présent document de travail.

Pratiquement parlant, ce sont surtout les sociétés multinationales qui devraient recourir le plus souvent à ces mécanismes pour réglementer les transferts internationaux entre leurs différentes filiales. Le groupe de travail «Article 29» souhaite insister à nouveau sur le fait que la portée de toute autorisation octroyée sur la base de cet instrument ne peut couvrir que les transferts ou catégories de transfert au sein du groupe, en d'autres termes, les échanges de données personnelles entre sociétés liées par ces règles d'entreprise. Les transferts de données personnelles vers des entreprises extérieures au groupe seraient toujours envisageables, non pas sur la base des dispositions de des règles d'entreprise contraignantes mais sur la base de tout autre instrument légitime au sens de l'article 26 de la directive (par ex. sur la base de contrats types de clauses contractuelles ou de contrats *ad hoc* conclus avec les destinataires des données).

3.2. Transferts ultérieurs

Les transferts ultérieurs, à savoir les transferts effectués à partir de filiales du groupe établies en dehors de la Communauté vers des entreprises extérieures à ce groupe, seraient possibles en cas d'acceptation des clauses contractuelles adoptées par la Commission dans ses décisions 2001/497/CE (transferts vers des responsables du traitement) et 2002/16/CE (transferts vers des sous-traitants) ou sur la base des conditions fixées par ces décisions.

Conformément à ces décisions, les transferts ultérieurs de données à caractère personnel vers un autre responsable du traitement établi dans un pays tiers n'offrant pas un niveau de protection adéquat ou non couverts par une décision de la Commission adoptée conformément à l'article 25 (6) de la directive peuvent être autorisés si les personnes concernées ont, dans le cas de catégories spéciales de données, indubitablement accepté le transfert ultérieur ou, dans les autres cas, la possibilité de s'y opposer.

Les informations minimales à fournir aux personnes concernées devraient contenir dans un langage qui leur soit compréhensible:

- l'objectif du transfert ultérieur;

- l'identification de l'exportateur de données établi dans la Communauté, d'où proviennent les données à caractère personnel;

- les catégories des destinataires ultérieurs des données et les pays de destination;

- une remarque expliquant que, après le transfert ultérieur, les données peuvent être traitées par un responsable du traitement non lié par les règles d'entreprise contraignantes et établi dans un pays qui ne présente pas un niveau approprié de protection de la vie privée des personnes.

Les contrôles réguliers prévus au chapitre 4.4 des règles d'entreprise contraignantes devraient comprendre un volet spécial sur les transferts ultérieurs dans lequel sera examinée l'utilisation faite par le groupe des contrats types. Le groupe devrait communiquer, sur demande, ces contrats aux autorités de protection des données et aux personnes concernées en respectant les conditions visées dans les décisions de la Commission susmentionnées.

3.3. Considérations à propos du caractère contraignant des règles d'entreprise

Les organisations répondent à leurs besoins de traitement de données en fonction de leurs contextes juridiques et culturels ainsi que de leurs philosophies et pratiques d'entreprise. Comme ces instruments ne bénéficient pas encore d'une grande expérience, il est évident que quasiment chaque multinationale aborde cette question d'une manière différente. Toutefois, un élément doit être commun à tous les systèmes si l'on veut que ceux-ci fournissent les garanties requises pour les transferts de données vers des pays tiers: à savoir le caractère **contraignant** des règles applicables aux entreprises à la fois à l'intérieur et à l'extérieur de celles-ci (caractère juridiquement exécutoire des règles).

3.3.1. Caractère contraignant des règles d'entreprise au sein du groupe[7]

Une distinction peut être établie entre le problème du respect des règles et le problème lié à leur caractère juridiquement exécutoire.

En effet, l'évaluation du «caractère contraignant» de ces règles d'entreprise implique une évaluation commune de leur nature contraignante tant *en droit (caractère juridiquement exécutoire)* qu'*en pratique (conformité interne à l'entreprise)*. Même si l'on peut, conceptuellement parlant, démontrer le caractère juridiquement exécutoire de ces engagements unilatéraux ou de contrats créant les mêmes effets, faire valoir ses droits dans une configuration transfrontalière s'avère en réalité toujours très complexe et peut exiger des efforts disproportionnés de la part des personnes concernées. Dès lors, il importe non seulement de veiller à ce que ces règles internes soient exécutoires d'un point de vue juridique mais également d'un point de vue pratique[8].

Le caractère contraignant des règles, *dans la pratique,* implique donc que les filiales du groupe, ainsi que chaque employé de celui-ci, se sentiront obligés de se conformer aux règles internes. À cet égard, divers éléments s'avèrent pertinents, comme l'application de sanctions disciplinaires en cas d'infraction aux règles, une information personnalisée et efficace aux employés, la mise en place de formations spéciales s'adressant aux employés et aux sous-traitants, etc. Tous ces éléments, également repris au point 5, pourraient expliquer le fait que les personnes au sein du groupe se sentent obligées de respecter ces règles.

D'un point de vue interne, il n'incombe pas au groupe de travail de déterminer comment les groupes doivent s'y prendre pour veiller à ce que toutes leurs filiales soient effectivement liées par les règles ou se sentent tenues vis-à-vis de celles-ci, même si certains exemples sont bien connus en la matière, comme c'est le cas de politiques internes dont l'application relève du siège central ou de codes de conduite internes étayés par des conventions internes à l'entreprise.[9] Ceci dit, les groupes ne doivent pas oublier

---

[7] L'adoption d'un code de conduite est une mesure que les multinationales ne prennent pas à la légère car elle implique des risques non négligeables, voire des conséquences juridiques, pour les sociétés qui enfreignent leur propre code.

[8] Le document WP 12 met en évidence une approche fonctionnelle et soutient que le facteur déterminant, ce qui concerne l'offre d'un niveau de protection adéquat, est d'assurer ce niveau de protection sur le plan pratique.

[9] Idéalement, les règles d'entreprise contraignantes devraient être adoptées par le conseil d'administration de la maison mère du groupe.

que ceux qui sollicitent une autorisation devront prouver à l'autorité qui l'octroie que cela est effectivement le cas à travers l'ensemble du groupe.

Le caractère contraignant des règles, sur le plan interne, doit être suffisamment clair et pertinent de manière à garantir le respect des règles en dehors de la Communauté, normalement sous la responsabilité du siège européen ou de la filiale européenne responsable par délégation de la protection des données, qui doit prendre toutes les mesures nécessaires pour garantir que chaque filiale étrangère adapte ses opérations de traitement en fonction des dispositions visées dans les règles d'entreprise contraignantes.[10]

En effet, il existe toujours une filiale du groupe implantée dans l'UE qui fournit les garanties nécessaires et qui introduit la demande d'autorisation auprès de l'autorité de protection des données. Si le siège du groupe était implanté ailleurs, celui-ci devrait déléguer cette responsabilité à une filiale établie au sein de l'Union européenne. Le fait que l'entité fournissant les garanties demeure responsable de la conformité aux règles et de leur application est tout à fait logique. Voir également à ce propos les chapitres 5.5 et 5.6 concernant la responsabilité et la juridiction.

3.3.2. Contrôle du caractère juridiquement exécutoire des règles d'entreprise par les personnes concernées (droits de tiers bénéficiaires) et les autorités de protection des données

Les personnes concernées couvertes par les règles d'entreprise contraignantes doivent devenir des tiers bénéficiaires par le biais soit des effets légaux des engagements unilatéraux (lorsque cela est possible, dans le cadre de la législation nationale), soit des dispositions contractuelles entre les membres du groupe qui le permettent. En tant que tiers bénéficiaires, les personnes concernées doivent pouvoir faire respecter ces règles en introduisant une plainte aussi bien auprès de l'autorité compétente de protection des données qu'auprès du tribunal compétent sur le territoire de la Communauté, comme cela est expliqué plus loin au chapitre 5.6.

Pour le groupe de travail «Article 29», il est capital que ces deux possibilités existent. Quoiqu'il semble plus facile en principe pour les personnes concernées d'introduire une plainte auprès de l'autorité compétente de protection des données - et, en effet, le devoir que le groupe a de coopérer avec l'autorité est susceptible de résoudre la plupart des problèmes - deux raisons justifient encore, même à supposer que le système fonctionne bien, le droit de saisir la justice (cf. chapitre 5.6):

a) l'obligation de coopération ne peut jamais garantir le respect à 100 % des règles et les personnes concernées ne sont pas nécessairement d'accord avec l'avis de l'autorité de protection des données, et

b) la compétence des autorités de protection des données au sein de la Communauté peut varier légèrement d'un pays à l'autre (certaines ne sont par exemple pas directement compétentes pour imposer des sanctions ou pour bloquer des transferts) et aucune d'elles ne peut accorder de dommages-intérêts, seuls les tribunaux jouissant de cette prérogative.

---

[10] En vertu du droit international des sociétés, des filiales peuvent être amenées s'imposer des codes de conduite les unes aux autres en cas d'allégations de violation quasi-contractuelle, de fausse déclaration et de négligence.

Si la possibilité pour les personnes concernées de faire respecter les règles en recourant à la justice constitue un élément nécessaire pour les raisons qui viennent d'être exposées, le groupe de travail «Article 29» attache encore plus d'importance à l'application pratique de ces règles par le groupe, dans la mesure où il s'agit là de la finalité de toute approche fondée sur l'autoréglementation.

Par ailleurs, les différences entre droit civil et droit administratif posent la question de savoir si des engagements unilatéraux peuvent ou non être considérés comme une base juridiquement valable à une clause de tiers bénéficiaire (stipulation pour autrui).

Alors que dans certains cas le caractère juridiquement exécutoire de ces engagements unilatéraux paraît clair, la situation est plus vague dans d'autres États membres et ces engagements unilatéraux risquent dès lors de ne pas s'avérer suffisants. Là où les engagements unilatéraux ne constituent pas une base juridique valable à une clause de tiers bénéficiaire, les groupes devraient mettre en place les conventions contractuelles nécessaires pour que les tiers puissent se prévaloir de tels droits. Ces engagements doivent avoir des effets juridiques valables en vertu du droit privé de chacun des États membres.[11]

La portée des droits liés au statut de tiers bénéficiaire correspondra au moins à celle prévue par la décision 2001/497/CE de la Commission relative aux clauses contractuelles types, tant vis-à-vis de l'exportateur de données que de l'importateur de données (cf. clause 3 «tiers bénéficiaire»[12]): cela confirme la valeur et l'importance des clauses contractuelles types actuellement en vigueur.

---

[11] Aujourd'hui, des droits de tiers bénéficiaires peuvent être octroyés par contrat dans l'ensemble des États membres. Cf. à ce propos les expériences précédentes en matière de clauses contractuelles types et de tiers bénéficiaires.

[12] Les personnes concernées seront habilitées à faire respecter les droits suivants (pour plus de facilité, les clauses correspondantes de la décision de la Commission relative aux clauses contractuelles types sont indiquées entre parenthèses):

- si le transfert porte sur des catégories spéciales de données, les personnes concernées ont été informées ou seront informées avant le transfert que leurs données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat (clause 4b)

- les personnes concernées obtiendront, si elles le demandent, une copie des règles d'entreprise contraignantes (clauses 4c et 5e)

- obtenir une réponse, dans des délais raisonnables et dans la mesure du possible, aux demandes de renseignements relatives au traitement de ces données personnelles en dehors de la Communauté (clauses 4d et 5c)

- faire savoir qu'une filiale du groupe liée par les règles ne coopère pas avec l'autorité compétente de protection des données et/ou ne suit pas les conseils de cette dernière en ce qui concerne le traitement des données transférées (clause 5c)

- faire savoir que la législation applicable à toute filiale d'un groupe, quel qu'il soit, en dehors de la Communauté, l'empêche de remplir ses obligations au titre des règles d'entreprise contraignantes (clause 5a)

- faire savoir que le traitement des données personnelles de toute filiale du groupe liée aux règles n'est pas conforme aux règles d'entreprise contraignantes (clause 5b)

Ces arrangements contractuels ne doivent pas nécessairement être complexes ou longs. Ils ne servent qu'à offrir aux personnes un statut de tiers bénéficiaire dans les pays où l'on doute que les déclarations unilatérales puissent permettre d'aboutir à un tel résultat. Dans certains cas, il suffirait d'insérer une clause dans d'autres contrats conclus entre les filiales du groupe. Par exemple, là où des contrats ont été conclus entre le siège et les filiales dans le but de garantir le respect des règles d'entreprise contraignantes au niveau interne - voir chapitre précédent - l'inclusion d'une «clause de tiers bénéficiaire» suffirait à satisfaire à cette exigence.

En ce qui concerne le contrôle du caractère juridiquement exécutoire des règles d'entreprise contraignantes par l'autorité compétente de protection des données, il est évident qu'en introduisant une demande d'autorisation de transfert international de données, le groupe s'engage, vis-à-vis de l'autorité de protection des données, à respecter les garanties fournies (en l'occurrence les règles d'entreprise contraignantes). Pour autant, cela ne préjuge en rien de la question de savoir si la responsabilité de faire respecter ce type d'engagement incombe à l'autorité chargée de la protection des données elle-même ou à toute autre instance (comme par exemple un tribunal, sur le conseil de l'autorité de protection des données).

En outre, les personnes concernées peuvent toujours introduire une plainte auprès de l'autorité nationale de protection des données ou d'un tribunal, tel que spécifié au chapitre 5.6 ci-dessous. Cette solution peut s'avérer plus satisfaisante pour les personnes concernées et, en tous les cas, leur offrir une sorte de statut «indirect» de tiers bénéficiaire.

3.3.3. Exigences de la législation nationale applicable aux filiales du groupe

Les règles d'entreprise contraignantes doivent clairement stipuler que lorsqu'une filiale du groupe a des raisons de penser que la législation qui lui est applicable risque de l'empêcher de remplir ses obligations en vertu des règles d'entreprise contraignantes et d'avoir un impact négatif sur les garanties fournies, ladite filiale en informera immédiatement le siège européen du groupe ou la filiale européenne responsable par délégation de la protection des données, à moins que cela ne soit interdit par une autorité chargée d'assurer le respect de la loi, comme par exemple une interdiction prévue par le code pénal pour préserver le secret de l'instruction.

- faire jouer la responsabilité et, le cas échéant, obtenir réparation conformément aux dispositions visées dans les règles d'entreprise contraignantes (clause 6)

- recourir à une juridiction européenne conformément aux dispositions visées dans les règles d'entreprise contraignantes (clause 7)

- faire savoir que les règles ont été modifiées au mépris des règles d'entreprise contraignantes ou des obligations qui en découlent en termes de procédure, ou que toute filiale du groupe n'honore pas ses obligations une fois qu'elle n'est plus liée par les règles (clauses 9 et 11)

La portée des droits liés au statut de tiers bénéficiaire doit apparaître clairement dans les dispositions contractuelles qui en sont à l'origine.

Le siège européen ou la filiale européenne responsable par délégation de la protection des données devraient prendre une décision responsable et consulter les autorités compétentes de protection des données. Toute incidence liée à ce chapitre des règles sera détaillée et examinée par les audits réguliers prévus au chapitre 5.2.

Les exigences de la législation nationale applicable aux filiales du groupe qui ne vont pas au-delà de ce qui est nécessaire au sein d'une société démocratique, sur la base de l'un des intérêts énumérés dans l'article 13 (1) de la directive 95/46/CE[13], ne vont en principe pas à l'encontre des règles d'entreprise contraignantes. Parmi certains exemples d'exigences qui ne vont pas au-delà de ce qui est nécessaire au sein d'une société démocratique, citons notamment les sanctions reconnues au niveau international, l'obligation de déclaration fiscale ou l'obligation d'information en matière de lutte contre le blanchiment d'argent. En cas de doute, les groupes consulteront sans tarder les autorités compétentes chargées de la protection des données.

4. CONTENU SUBSTANTIEL DES RÈGLES D'ENTREPRISE CONTRAIGNANTES

4.1. Contenu substantiel et niveau de détail

Le groupe de travail réaffirme les principes contenus dans le document de travail n° 12[14], plus particulièrement en son chapitre 3 (*Application de l'approche aux codes d'autoréglementation sectoriels*) et, dans une moindre mesure, en son chapitre 6 (*Questions de procédure*). Il faut cependant admettre que ces principes ne signifient en soi pas grand-chose pour les sociétés et les employés s'occupant du traitement des données personnelles en dehors de la Communauté, en particulier dans les pays qui ne disposent pas de législation dans ce domaine ni, selon toute vraisemblance, d'aucune culture de protection des données, quelle qu'elle soit.

Ces principes doivent être développés et détaillés dans le cadre de règles d'entreprise contraignantes, afin de pouvoir s'adapter de manière pratique et réaliste aux opérations de traitement effectuées par l'organisation dans des pays tiers, et être compris et appliqués effectivement par les responsables chargés de la protection des données au sein de l'organisation.

En considérant les choses sous cet angle, l'on peut trouver un dénominateur commun entre les règles d'entreprise contraignantes et les codes de conduite visés à l'article 27 de la directive, dans le sens où elles sont supposées dépasser le degré d'abstraction de la législation (en l'occurrence les principes contenus le document de travail n° 12). Les

---

[13] C'est-à-dire si elles constituent des mesures nécessaires pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées, un intérêt économique ou financier important d'un État membre ou la protection de la personne concernée ou des droits et libertés d'autrui.

[14] Document de travail: Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données.

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.pdf

règles d'entreprise devraient comporter des dispositions «sur mesure» et décrire de manière raisonnablement détaillée les flux de données, la finalité du traitement, etc.

Comme l'indique l'article 26 (2) de la directive, l'autorisation peut porter sur un transfert ou un ensemble de transferts; mais dans tous les cas les transferts autorisés doivent être expliqués. Le niveau de détail doit être suffisant afin de permettre aux autorités de protection des données d'évaluer le caractère adéquat du traitement effectué dans des pays tiers (p. ex. une description détaillée des activités économiques menées par les différentes entités du groupe).

À titre d'exemple et pour autant que la législation nationale applicable prévoie un système de notification, on pourrait suggérer, d'un point de vue pratique, que dans les pays où le système de notification est très détaillé, cette partie des règles d'entreprise contraignantes reflète les règles concernant les modalités de notification que les responsables du traitement doivent respecter vis-à-vis des autorités de protection des données: tout comme la notification permet à l'autorité chargée de la protection des données de comprendre les opérations menées à bien par le responsable du traitement[15], le même niveau d'information devrait en principe s'avérer suffisant pour permettre à l'autorité de protection des données de comprendre les opérations de traitement couvertes par les règles d'entreprise contraignantes au sein du groupe. Là où le système de notification n'est pas suffisamment détaillé (l'article 18 (2) de la directive offre une grande marge de manœuvre à cet égard aux États membres), un complément d'information s'imposera en vue de fournir une description pertinente des données à caractère personnel transférées vers des pays tiers. Les règles d'entreprise contraignantes ne remplacent en aucune façon l'obligation de notification visée dans la législation de l'UE.

4.2. Particularisation et mise à jour des règles

Les règles d'entreprise contraignantes peuvent affiner les règles applicables à différents pays ou différentes régions en dehors de la Communauté si tel est le souhait du groupe qui les met en œuvre. Toutefois, cette particularisation risque de toute évidence de rendre le système plus complexe, alors que l'objectif de ce dernier est de concevoir des politiques globales.

S'agissant de la mise à jour des transferts effectués et, automatiquement, de la mise à jour des règles, le groupe de travail «Article 29» admet que groupes sont des entités en mutation dont les filiales et les pratiques peuvent changer de temps en temps et qui, partant, ne peuvent correspondre à 100 % à la réalité en vigueur au moment de l'octroi de l'autorisation. Les mises à jour sont possibles (sans devoir réintroduire une nouvelle demande d'autorisation) si les conditions suivantes sont remplies:

a) aucun transfert de données personnelles n'est effectué vers une nouvelle filiale tant que l'exportateur des données ne s'est pas assuré que cette nouvelle filiale est effectivement liée par les règles en question et qu'elle est en mesure de les respecter;

b) une personne ou un département désignés au sein du groupe doit tenir une liste des filiales totalement mise à jour et garder trace et consigner toute mise à jour des règles et

[15] Cf. article 19 de la directive.

fournir les informations requises aux personnes concernées ou aux autorités de protection des données, à leur demande;

c) toute mise à jour des règles ou modification de la liste des filiales doit être notifiée une fois par an aux autorités chargées de la protection des données octroyant les autorisations, assortie d'un bref exposé des motifs justifiant cette mise à jour.

La mise à jour des règles sous-entend l'évolution éventuelle des procédures de travail et, partant, la nécessité d'adapter ces règles à ces environnements en mutation. Toute modification importante portant non seulement sur les principes de protection mais également sur les finalités du traitement, les catégories de données traitées ou les catégories de personnes concernées peut en principe avoir un impact sur l'autorisation.

5. GARANTIES DE CONFORMITÉ ET DE MISE EN APPLICATION INTERNE

Outre ces principes substantiels en matière de protection des données, toutes règles d'entreprise contraignantes applicables aux transferts internationaux de données doit contenir également:

5.1. Dispositions garantissant un bon niveau de conformité

Les règles sont censées instaurer un système qui garantit la transparence et la mise en œuvre de ces règles tant à l'intérieur qu'à l'extérieur de l'Union européenne. L'élaboration par le siège d'un groupe de mesures internes en matière de protection de la vie privée ne peut être considérée que comme un premier pas vers la présentation de garanties suffisantes au sens de l'article 26 (2) de la directive. Le groupe demandeur doit également être à même de prouver que cette politique est connue, comprise et effectivement appliquée, à travers l'ensemble de celui-ci par les employés formés en conséquence et disposant de toute l'information pertinente à tout moment, par exemple via l'intranet. Le groupe aura pour mission de désigner le personnel nécessaire, avec l'aide de la direction, afin de superviser et de garantir la conformité.

5.2. Audits

Les règles doivent prévoir des audits internes et/ou externes réalisés régulièrement par des contrôleurs agréés, qui transmettront un rapport directement au conseil d'administration de la maison mère du groupe[16]. Les autorités de protection des données recevront une copie de ces audits lorsque des mises à jour des règles sont notifiées et sur demande, le cas échéant, dans le cadre de la coopération avec l'autorité de protection des données.

Les règles doivent également stipuler que le devoir de coopérer avec les autorités de protection des données (cf. chapitre 5.4) peut exiger la réalisation d'audits par des inspecteurs de l'autorité de contrôle même ou par des auditeurs indépendants au nom de l'autorité de contrôle. Cela risque vraisemblablement de se produire lorsque les audits

---

[16] Le contenu de ces contrôles sera exhaustif et décrira en détail les points particuliers déjà identifiés dans le présent document de travail, tels que l'existence de transferts ultérieurs sur la base de clauses contractuelles types (cf. chapitre 3.2) ou les décisions prises en ce qui concerne les exigences de la législation nationale pouvant aller à l'encontre des règles d'entreprise contraignantes (cf. chapitre 3.3.3).

prévus dans le paragraphe précédent ne sont pas disponibles pour l'une ou l'autre raison, lorsqu'ils ne contiennent pas les informations pertinentes nécessaires à un suivi normal de l'autorisation octroyée ou lorsque l'urgence de la situation plaide en faveur d'une participation directe de l'autorité compétente de protection des données ou de contrôleurs indépendants en son nom.

Ces audits seraient menés conformément à la législation et aux réglementations régissant les pouvoirs d'investigation des autorités chargées de la protection des données, sans préjuger en aucune façon des pouvoirs d'inspection de chaque autorité de protection des données; audits dont le groupe sera averti en temps opportun par l'autorité compétente de protection des données. En tous les cas, ils seront effectués dans le respect total de la confidentialité et du secret des affaires et devront être ciblés uniquement sur la vérification du respect des règles d'entreprise contraignantes.

5.3. Gestion des plaintes

Les règles doivent instaurer un système de gestion des plaintes individuelles au sein d'un département clairement identifié. Les responsables chargés de la protection des données ou toute personne responsable de la gestion des plaintes doivent pouvoir jouir d'un degré approprié d'indépendance dans l'exercice de leurs fonctions. Le recours à des mécanismes alternatifs de résolution des litiges, avec une éventuelle participation des autorités de protection des données, le cas échéant, devra également être favorisé, dans le respect des législations et réglementations nationales applicables.

5.4. Le devoir de coopération avec les autorités de protection des données

Tel qu'indiqué dans le document WP 12, l'un des critères les plus importants servant à évaluer le niveau de protection adéquat d'un système d'autoréglementation est le degré de soutien et d'assistance offert aux personnes concernées:

«Une exigence essentielle à laquelle doit répondre un système de protection des données approprié et efficace est qu'une personne physique confrontée à un problème touchant aux données personnelles la concernant ne soit pas laissée à elle-même, mais puisse bénéficier d'un soutien institutionnel pour la solution de ses problèmes»

Il s'agit là en effet de l'un des éléments les plus importants des règles d'entreprise contraignantes applicables aux transferts internationaux de données: les règles doivent clairement faire état du devoir de coopération avec les autorités de protection des données, de façon à ce que les particuliers puissent bénéficier du soutien institutionnel visé dans le document WP 12.

Il faut qu'il soit clairement entendu que le groupe dans son ensemble et chacune de ses filiales, séparément, acceptent les conditions des contrôles visées dans le chapitre 5.2. Il faut qu'il soit également clairement entendu que le groupe dans son ensemble et chacune de ses filiales, séparément, respectent les conseils de l'autorité compétente chargée de la protection des données pour tout ce qui touche à l'interprétation et à l'application de ces règles d'entreprise contraignantes. Les conseils de l'autorité compétente chargée de la protection des données prendront la forme de recommandations adressées au groupe, soit en réponse à un questionnaire, à une plainte introduite par une personne concernée ou à la propre initiative de l'autorité chargée de la protection des données.

Avant de formuler tout conseil, l'autorité compétente de protection des données peut solliciter l'avis du groupe, des personnes concernées ainsi que des autorités de protection des données susceptibles d'être associées au processus du fait de la procédure de coopération prévue dans le présent document de travail[17]. Les conseils de l'autorité peuvent être rendus publics.

Outre toute disposition pertinente au niveau national, si le groupe refuse fermement et persiste à refuser de coopérer ou de se conformer aux conseils de l'autorité compétente de protection des données, l'autorisation octroyée par cette dernière ou par l'instance compétente dûment habilitée à le faire en vertu de la législation nationale pourra être suspendue ou lui être retirée. Cette décision prendra la forme d'un acte administratif que le destinataire pourra contester en introduisant une action auprès du tribunal compétent, conformément à la législation nationale en vigueur. Elle sera notifiée à la Commission européenne ainsi qu'aux autres autorités de protection des données concernées et pourra également être rendue publique.

5.5. Responsabilité

5.5.1. Droit général visant à obtenir réparation, voire compensation, le cas échéant

Les règles stipuleront que les personnes concernées bénéficieront des droits en matière de réparation et de responsabilité visés aux articles 22 et 23 de la directive (ou de disposition similaires transposant ces articles de la directive dans les législations des États membres), dans les mêmes conditions et dans la même mesure que si le traitement effectué par le groupe relevait du champ d'application de la directive relative à la protection des données ou de toute législation nationale transposant celle-ci.

La finalité de ces règles se limite donc à assurer que les autorisations délivrées par les autorités de protection des données (qui permettront ou légaliseront un transfert de données personnelles vers l'étranger qui, sans quoi, s'avérerait illicite) n'hypothèquent pas le droit des personnes concernées à obtenir réparation ou compensation, comme cela aurait été le cas si les données n'avaient pas quitté le territoire de l'UE.[18]

Afin de compléter ce droit général et d'en faciliter l'exercice sur le plan pratique, les règles doivent également contenir des dispositions en matière de responsabilité et de juridiction.

5.5.2. Dispositions en matière de responsabilité

---

[17] Cf. chapitre 6.

[18] Par le passé, certaines multinationales ont rechigné à adopter des politiques globales en matière de respect de la vie privée invoquant le fait que, bien qu'elles puissent accepter d'assurer un niveau de protection adéquat dans des régions couvertes par la législation européenne, elles se refusaient cependant à offrir le même niveau de protection à des pays ou régions où ce niveau se révélait inférieur ou nul. Elles ont toujours manifesté une certaine inquiétude face à l'inclusion de dispositions visant à permettre aux personnes concernées d'obtenir réparation ou une compensation. La présente formulation vise à effacer cette inquiétude parce que, comme expliqué au chapitre 3.1, le champ d'application des règles d'entreprise contraignantes (y compris donc la réparation des dommages) peut être limité aux données originaires de l'UE.

Tout d'abord, le siège (si établi dans l'UE) ou la filiale européenne responsable par délégation de la protection des données devraient accepter d'endosser la responsabilité et de prendre les mesures nécessaires pour réparer les actes commis par d'autres filiales du groupe situées en dehors la Communauté et, le cas échéant, de verser une compensation (dans les conditions énoncées dans le chapitre précédent) pour tout préjudice résultant de la violation des règles d'entreprise contraignantes par l'une ou l'autre filiale liée par celles-ci.

Le groupe accompagnera sa demande d'autorisation des pièces prouvant que le siège européen ou la filiale européenne responsable par délégation de la protection des données disposent de ressources financières en suffisance au sein de la Communauté pour couvrir le versement d'une compensation du fait de la violation des règles d'entreprise contraignantes dans un contexte normal, ou que des mesures ont été prises pour pouvoir faire face à ce type de réclamations (par exemple: souscription d'une assurance en responsabilité).

Le siège (si établi dans l'UE) ou la filiale européenne responsable par délégation de la protection des données doivent également accepter d'être poursuivis dans l'Union européenne et, le cas échéant, de verser des indemnités:

a) en cas de demande de dédommagement suite à la violation des règles d'entreprise contraignantes, ou

b) lorsque aucune demande de dédommagement n'a été introduite mais que la personne concernée n'est pas satisfaite de la réparation obtenue par le biais des procédures internes de gestion des plaintes (cf. chapitre 5.3) ou par le biais de l'introduction d'une plainte auprès de l'autorité compétente chargée de la protection des données.

Si le siège européen ou la filiale européenne responsable par délégation de la protection des données sont en mesure de prouver que la filiale du groupe située dans un pays tiers n'est pas responsable de l'acte ayant conduit au préjudice dénoncé par la personne concernée, il ou elle sera dégagé(e) de toute responsabilité.

Les règles devraient stipuler que qu'il revient toujours au siège européen ou à la filiale européenne responsable par délégation de la protection des données de démontrer que la filiale du groupe à l'extérieur de la Communauté n'est pas responsable de l'infraction ayant conduit au préjudice dénoncé par la personne concernée plutôt qu'à cette dernière de prouver qu'une société établie dans un pays tiers effectue des opérations de traitement contraires aux règles d'entreprise (une preuve qui la plupart du temps serait impossible à matérialiser et qui, de toute façon, supposerait des efforts et un investissement en temps et en argent disproportionnés de la part de la personne concernée).

5.6. Dispositions en matière de juridiction

Tel qu'exposé dans le chapitre 5.5.2 ci-dessus, le groupe doit également accepter que les personnes concernées aient le droit d'intenter une action contre le groupe et de choisir la juridiction:

a) soit la juridiction dont relève la filiale à l'origine du transfert, ou

b) la juridiction dont relève le siège ou la juridiction dont relève la filiale européenne responsable par délégation de la protection des données.

À supposer que le système fonctionne de manière adéquate et, par conséquent, que le niveau de conformité soit satisfaisant dans l'ensemble du groupe, que des audits aient lieu régulièrement, que le système de gestion des plaintes soit efficace et qu'il y ait une coopération avec les autorités de protection des données…, le recours devant les tribunaux apparaît comme improbable mais ne peut en aucun cas être exclu. Cela étant dit, seule l'expérience démontrera le bien-fondé de cette prévision.

S'appliqueront alors les principes et règles pertinents en matière de juridiction contenus à la fois dans la directive et dans les différentes législations nationales.

5.7. Transparence

Outre les informations à fournir en vertu des articles 10 et 11 de la directive et de la législation nationale les transposant, les groupes qui offrent des garanties suffisantes doivent être en mesure de démontrer que les personnes concernées sont au courant de la communication de leurs données personnelles à d'autres filiales du groupe à l'extérieur de la Communauté, conformément aux autorisations délivrées par les autorités de protection des données sur la base de règles d'entreprise juridiquement exécutoires, lesquelles doivent être portées à la connaissance des personnes et aisément accessibles par celles-ci.

Cette obligation de fournir des informations détaillées signifie que, sans porter préjudice aux règles d'entreprise dans leur ensemble, les groupes doivent être en mesure de prouver que les personnes ont facilement accès aux informations relatives aux principaux engagements pris par le groupe en matière de protection des données, aux informations actualisées concernant les filiales liées par les règles ainsi qu'aux moyens mis à la disposition des personnes concernées pour vérifier le respect de ces règles.

6. PROCÉDURE DE COOPÉRATION ENTRE AUTORITÉS NATIONALES DANS LE CADRE DES DEMANDES D'AUTORISATION VISÉES À L'ARTICLE 26 (2) DE LA DIRECTIVE

Le groupe de travail est conscient de l'importance de la notification de toute autorisation adressée aux États membres et à la Commission européenne, comme le prévoit l'article 26 (3) de la directive. Ces notifications peuvent toutefois s'accompagner d'activités complémentaires de coopération entre les autorités nationales de protection des données avant l'octroi des autorisations en question. Cette coopération est d'ailleurs prévue par l'article 28 de la directive, dans les cas où une décision prise au niveau national risque d'avoir une incidence sur les opérations de traitement du même groupe dans un autre État membre.

Les groupes qui souhaitent obtenir une licence pour des types similaires de transfert de données, à partir de plusieurs États membres, peuvent utiliser une procédure coordonnée[19]. Toute activité coordonnée s'applique uniquement aux autorités de protection des données habilitées, en vertu du droit national, à autoriser des transferts internationaux de données et légalement en mesure d'accepter d'être impliquées de temps à autres et au cas par cas.

L'idée principale qui sous-tend ces dispositions de procédure est de permettre à une entreprise de n'introduire qu'une seule demande d'autorisation auprès d'une autorité de protection des données d'un État membre, ce qui conduira, via le processus de coordination en place entre les autorités de protection des données concernées, à l'octroi d'autorisations par l'ensemble des différentes autorités de contrôle des États membres où l'entreprise en question développe ses activités. Les détails de la procédure seront alors établis sans délai au cas par cas par les autorités de protection des données impliquées.

Le présent document de travail ne porte pas atteinte aux droits et obligations que les autorités nationales de contrôle tiennent en vertu de leur législation nationale de considérer les plaintes des individus et, en général, de suivre l'application de la directive dans les cas où elles sont compétentes. Ces dispositions offrent cependant une réponse au devoir de coopération prévu à l'article 28 (6) de la directive dans les cas où elles sont tenues, en vertu des prescriptions nationales, de collaborer entre elles.

---

[19] Le groupe de travail «Article 29» devrait être en mesure de fournir davantage de détails sur cette question, dans un avenir très proche, sur la base de l'expérience acquise avec ladite procédure. Il existe des relations de travail basées sur la coopération entre les autorités de contrôle des États membres et, dès lors, il est inutile de parer à toute éventualité. Le demandeur est tenu de mentionner le point d'entrée retenu, en expliquant les raisons de ce choix et en précisant les autres autorités nationales de contrôle impliquées dans la procédure. L'octroi des autorisations requises conformément à l'article 26 (2) de la directive et aux réglementations nationales qui en découlent, ainsi que la notification à la Commission européenne, constitueront les étapes finales de cette procédure coordonnée.

7. CONCLUSION

Le groupe de travail estime que les orientations contenues dans le présent document peuvent faciliter l'application de l'article 26 (2) de la directive. Elles devraient également simplifier la tâche des groupes multinationaux qui ont l'habitude d'échanger des données personnelles à l'échelon mondial.

Le contenu du présent document de travail ne doit pas être considéré comme l'avis définitif du groupe de travail «Article 29» sur cette question, mais plutôt comme un premier élément décisif visant à encourager l'utilisation d'autorisations nationales, conformément à l'article 26 (2), et reposant sur une approche axée sur l'autoréglementation et sur la coopération entre les différentes autorités compétentes, et cela sans porter préjudice à la possibilité de recourir à d'autres instruments aux fins du transfert de données personnelles vers l'étranger, tels que les clauses contractuelles types ou les principes de la «sphère de sécurité», le cas échéant.

Toutes les contributions des acteurs intéressés et des experts, à la lumière des expériences acquises grâce à l'utilisation du présent document de travail, sont les bienvenues. Le groupe de travail se réserve le droit de réexaminer cette question à lumière de l'expérience acquise.

Fait à Bruxelles, le 3 juin 2003
Par le groupe de travail
Le Président
Stefano RODOTA