Groupe de travail «Article 29» sur la protection des données

**1271-00/08/FR**
**WP 153**

# Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes

**Adopté le 24 juin 2008**

## INTRODUCTION

Afin de faciliter l'application des règles d'entreprise contraignantes (BCR) par les groupes d'entreprises dans le cadre des transferts internationaux qu'ils effectuent de l'UE vers leurs filiales, le groupe de travail «Article 29» a élaboré le tableau ci-après dont l'objectif est:

- de préciser le contenu obligatoire des BCR tel qu'il est exposé dans deux documents distincts, à savoir le WP 74[1] et le WP 108[2],

- d'établir une distinction entre ce qui doit être inclus dans les BCR et ce qui doit être présenté aux autorités chargées de la protection des données dans le cadre d'une demande d'approbation des BCR (document WP 133[3]),

- pour chaque principe, d'indiquer des références aux documents WP 74[4] et WP 108[5] pour plus de détails, et

- de fournir des explications/commentaires sur chacun des principes.

---

1 Document de travail WP 74: 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 donnés aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, adopté le 3 juin 2003 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_fr.htm.

2 Document de travail WP 108 établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes, adopté le 14 avril 2005. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_fr.htm.

3 Document de travail WP 133: Recommandation 1/2007 relative au formulaire de demande d'approbation des règles d'entreprise contraignantes applicables au transfert des données à caractère personnel http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_fr.htm.

4 Cf. note de page 1.

5 Cf. note de page 2.

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| **1 – CARACTÈRE CONTRAIGNANT** | | | | |
| **EN INTERNE** | | | | |
| **1.1 L'obligation de respecter les BCR** | OUI | OUI | WP 74 point 3.3.1 (pages 10-11) + WP 108 point 5.3 à 5.9 (page 5) | Les BCR doivent clairement indiquer que toutes les filiales du groupe et les employés sont tenus de respecter les BCR. |
| **1.2 Une explication sur la manière dont les règles sont rendues contraignantes pour les filiales du groupe et les employés** | NON | OUI | WP 74 point 3.3.1 (pages 10-11) + WP 108 point 5.3 à 5.9 (page 5) | Dans son formulaire de demande, le groupe doit expliquer de quelle manière il confère aux règles un caractère contraignant:<br><br>i) entre les sociétés/entités au sein du groupe, par l'un ou plusieurs des moyens suivants:<br>accord intragroupe,<br>engagements unilatéraux,<br>mesures réglementaires internes,<br>politiques du groupe, ou<br>autres moyens;<br><br>ii) pour les employés, par l'un ou plusieurs des moyens suivants:<br>accord/engagement individuel et distinct, prévoyant des sanctions,<br>clause du contrat de travail prévoyant des sanctions,<br>politiques intérieures ou<br>conventions collectives prévoyant des sanctions. |
| **EN EXTERNE** | | | | |
| **1.3 Création de droits de tiers bénéficiaires pour les personnes concernées, avec la possibilité d'introduire une plainte aussi bien auprès des autorités de protection des données qu'auprès d'un tribunal (choix de la juridiction: tribunal de l'exportateur de données/ du siège européen/ de la filiale européenne responsable par délégation de la protection des données).** | OUI | OUI | WP 74 point 3.3.2. (pages 11-13), point 5.5.1. (page 18) et point 5.6 (page 19) + WP 108 points 5.12 à 5.14, point 5.16, point 5.20 (page 6) | Les BCR doivent garantir aux personnes concernées des droits en matière d'application des règles en qualité de tiers bénéficiaires. Parmi ces droits doivent figurer un droit de recours en cas de violation des droits garantis et un droit à réparation (voir articles 22 et 23 de la directive UE). |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| **1.4 La société accepte d'endosser la responsabilité d'une éventuelle indemnisation et de remédier aux infractions aux BCR.** | OUI | OUI | WP 74 point 3.3.1, § 5-6 (page 11), point 5.5.1 (page 18), point 5.5.2 (pages 18-19), point 5.6 (page 19) + W P108 point 5.17 (page 6) | Les BCR doivent imposer au siège européen, ou à la filiale européenne responsable par délégation de la protection des données, l'obligation d'endosser la responsabilité et de prendre les mesures nécessaires pour réparer les actes d'autres membres du groupe situés en dehors de l'UE et soumis à l'application des BCR, et de verser une indemnité pour tout préjudice résultant de la violation des BCR par l'un des membres.<br><br>Les BCR doivent également préciser que lorsqu'une filiale du groupe établie à l'extérieur de l'UE enfreint les BCR, ce cas relève de la compétence des tribunaux ou d'autres autorités compétentes au sein de l'UE. Les personnes concernées disposeront de droits et de recours juridictionnels contre la filiale qui aura endossé la responsabilité comme si l'infraction avait été commise par celle-ci dans l'État membre où elle est établie, en lieu et place de la filiale du groupe établie à l'extérieur de l'UE.<br><br>S'il n'est pas possible pour certains groupes, dont la structure d'entreprise est particulière, d'imposer à une entité d'assumer la totalité de la responsabilité à l'égard des violations des BCR à l'extérieur de l'UE, les autorités de protection des données peuvent accepter d'autres mécanismes de responsabilité définis au cas par cas, dans la mesure où ils permettent de s'assurer de façon satisfaisante que les personnes concernées pourront faire valoir leurs droits et qu'elles ne seront pas désavantagées lors de ce processus. Parmi les régimes possibles de responsabilité figurent le mécanisme de responsabilité solidaire entre importateurs et exportateurs de données prévu dans les clauses contractuelles types établies par la décision 2001/497/CE de la Commission du 15 juin 2001, ou le régime de responsabilité reposant sur des obligations de diligence telles que fixées dans les clauses contractuelles types visées dans la décision 2004/915/CE de la Commission du 27 décembre 2004. Une dernière possibilité, concernant en particulier les transferts effectués par des responsables du traitement vers des sous-traitants, consiste à appliquer le mécanisme de responsabilité |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| | | | | prévu dans les clauses contractuelles types visées dans la décision 2002/16/CE de la Commission du 27décembre 2001. |
| **1.5 La société dispose de ressources financières suffisantes.** | NON | OUI | WP 74 point 5.5.2 §2 (page 18) + WP 108 point 5.17. (page 6) | Le formulaire de demande doit confirmer que l'entité qui a accepté la responsabilité des actes d'autres membres liés par les BCR à l'extérieur de l'UE dispose de ressources financières suffisantes pour verser une indemnité par suite d'une violation des BCR. |
| **1.6 La charge de la preuve incombe à la société et non pas à l'individu.** | OUI | OUI | WP 74 point 5.5.2 § 6 et 7 (page 19) + WP 108 point 5.19 (page 6) | Les BCR doivent indiquer que c'est à l'entité qui a accepté la responsabilité qu'il revient de prouver que la filiale du groupe à l'extérieur de l'UE n'est responsable d'aucune violation des règles ayant entraîné une demande de réparation de la part de la personne concernée.<br><br>L'entité ayant accepté la responsabilité peut être exonérée de toute responsabilité si elle est en mesure de prouver que la filiale du groupe à l'extérieur de l'UE n'est pas responsable de l'acte. |
| **1.7 Les personnes concernées ont facilement accès aux BCR et notamment aux informations concernant les droits des tiers bénéficiaires pour les personnes concernées qui en bénéficient.** | OUI | NON | WP74 point 5.7 (page 19) | Les BCR doivent consacrer le droit des personnes concernées d'accéder aisément aux BCR.<br><br>Toutes les personnes concernées bénéficiant de droits de tiers bénéficiaires devraient également pouvoir accéder facilement à cette clause.<br><br>Par exemple, il pourrait être prévu dans les BCR que celles-ci soient publiées sur l'internet ou sur l'intranet (si les personnes concernées sont le personnel de la société). |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| **2 –EFFICACITÉ** | | | | |
| **2.1 L'existence d'un programme de formation adéquat** | OUI | OUI | WP 74 point 5.1 (page 16) + WP108 + points 5.8-5.9. (page 5) | Les BCR doivent indiquer qu'une formation adéquate y afférente sera dispensée au personnel ayant accès en permanence ou régulièrement aux données personnelles et associé à la collecte des données personnelles ou au développement d'outils de traitement des données personnelles.<br><br>Au cours de la procédure de demande, les autorités de protection des données qui évaluent les BCR peuvent réclamer des exemples et des explications sur le programme de formation; celui-ci devra être présenté dans la demande. |
| **2.2 L'existence d'un processus de traitement des plaintes concernant les BCR** | OUI | OUI | WP 74 point 5.3 (page 17) + WP 108 point 5.15 et 5.18 (page 6) | Les règles doivent instaurer un système interne de traitement des plaintes. Toute personne concernée doit pouvoir introduire une plainte indiquant qu'un membre du groupe ne respecte pas les règles.<br><br>Les plaintes doivent être traitées par un département ou une personne clairement identifié(e) disposant d'un degré approprié d'indépendance dans l'exercice de ses fonctions.<br><br>Le formulaire de demande doit indiquer de quelle manière les personnes concernées seront informées des étapes pratiques du système de réclamation, et notamment des éléments suivants:<br>- où déposer plainte,<br>- sous quelle forme,<br>- délai de réponse à la plainte,<br>- conséquences en cas de rejet de la plainte,<br>- conséquences si la plainte est jugée recevable,<br>- conséquences si les personnes concernées ne sont pas satisfaites par les réponses (droit d'introduire un recours auprès d'un tribunal/de l'autorité de protection des données). |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| **2.3 L'existence d'un programme d'audit couvrant les BCR** | OUI | OUI | WP 74 point 5.2 (page 16) + WP 108 point 6 (page 7) | Les BCR doivent imposer au groupe la réalisation d'audits en matière de protection des données à intervalles réguliers (par des contrôleurs internes ou externes agréés) ou sur demande expresse du délégué ou de l'instance chargé(e) de la protection des données personnelles (ou de toute autre instance compétente au sein de l'organisation).<br><br>Les BCR doivent indiquer que le programme d'audit couvre tous les aspects des BCR, y compris les méthodes visant à garantir la mise en œuvre des mesures correctives. En outre, les BCR doivent indiquer que le résultat sera communiqué au délégué ou à l'instance chargé(e) de la protection des données ainsi qu'au conseil d'administration de la maison mère du groupe.<br><br>Les règles doivent indiquer que les autorités de protection des données peuvent, sur demande, avoir accès aux résultats de l'audit et doivent accorder à celles-ci l'autorisation ou le pouvoir de mener elles-mêmes des audits sur la protection des données, si nécessaire.<br><br>Le formulaire de demande inclura une description du système d'audit. Par exemple:<br>- quelle entité (service au sein du groupe) décide du plan/programme d'audit,<br>- quelle est l'entité qui mènera l'audit,<br>- fréquence de l'audit (régulièrement ou sur demande spéciale du responsable de la protection des données),<br>- champ couvert par l'audit (par exemple les applications, systèmes informatiques, bases de données gérant des données personnelles, ou les transferts ultérieurs, les décisions prises en matière d'obligations nées du droit national en conflit avec les règles d'entreprise contraignantes, le réexamen des clauses contractuelles appliquées aux transferts en dehors du groupe (vers les responsables du traitement des |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| | | | | données ou les sous-traitants), les actions correctives, etc.),<br>- quelle est l'entité qui recevra les résultats des audits. |
| **2.4 La création d'un réseau de responsables de la protection des données ou d'employés qualifiés pour la gestion des plaintes, la surveillance et le contrôle du respect des règles.** | OUI | NON | WP 74 point 5.1 (page 16) et 5.3 (page 17) | Engagement à désigner le personnel nécessaire (tel qu'un réseau de responsables de la protection des données), assisté par la direction, afin de superviser et de garantir le respect des règles.<br><br>Brève description de la structure interne, du rôle et des compétences du réseau ou des responsables de la protection des données ou de la fonction similaire créée pour garantir la conformité aux règles. Par exemple, une note selon laquelle le haut responsable de la protection des données remplit une fonction de conseil auprès de l'organe de direction, traite les demandes des autorités de protection des données, établit des rapports annuels sur le respect des règles, garantit le respect des règles au niveau global., et selon laquelle les délégués à la protection des données peuvent être chargés de traiter des plaintes émanant des personnes concernées, de soumettre des rapports sur des questions importantes liées à la protection des données au haut responsable de la protection des données et de garantir le respect des règles au niveau local. |
| **3 –DEVOIR DE COOPÉRATION** | | | | |
| **3.1 Une obligation de coopérer avec les autorités de protection des données** | OUI | OUI | WP 74 point 5.4 (page 17) + WP 108 point 5.21 (page 7) | Les BCR doivent clairement mentionner l'obligation de coopérer avec les autorités de protection des données qui incombe à tous les membres du groupe, ainsi que l'obligation de se soumettre à tout audit effectué par celles-ci et de se conformer à leur avis sur toute question ayant trait aux règles. |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| **4 – DESCRIPTION DU TRAITEMENT ET DES FLUX DES DONNÉES** | | | | |
| **4.1 Une description des transferts couverts par les BCR** | OUI | OUI | WP 74 point 4.1 § 4 (page 14) + WP 108 point 7 (pages 7-8) | Les BCR doivent également contenir une description générale des transferts afin de permettre aux autorités de protection des données d'évaluer le caractère adéquat du traitement effectué dans des pays tiers et, plus précisément, concernant:<br>i) la nature des données transférées,<br>ii) les finalités du transfert/traitement,<br>iii) les importateurs/exportateurs des données dans l'UE et à l'extérieur de l'UE.<br><br>Certaines autorités de protection des données peuvent exiger une description plus détaillée des transferts. |
| **4.2 Une déclaration de la portée géographique et matérielle des BCR (nature des données, type de personnes concernées, pays)** | OUI | OUI | WP 108 point 7.1.1 et 7.2) (pages 7-8) | Les BCR doivent indiquer si elles sont applicables:<br>i) à toutes les données personnelles transférées depuis l'Union européenne à l'intérieur du groupe, OU<br>ii) à tous les traitements de données personnelles réalisés au sein du groupe.<br><br>Les BCR doivent également préciser la portée matérielle du transfert, et notamment le fait qu'elles s'appliquent aux données personnelles des employés, clients, fournisseurs et autres tiers dans le cadre des activités normales de la société. |
| **5 – MODALITÉS DE COMMUNICATION ET D'ENREGISTREMENT DES MODIFICATIONS** | | | | |
| **5.1 Une procédure de mise à jour des BCR** | OUI | OUI | WP 74 point 4.2 (page 15) + WP 108 point 9 (pages 8-9) | Les BCR peuvent être modifiées (*par exemple, pour prendre en compte les modifications de l'environnement réglementaire ou de la structure de la société*) mais elles doivent imposer l'obligation de communiquer les modifications à toutes les filiales du groupe et aux autorités de protection des données.<br><br>Les mises à jour des BCR ou de la liste des filiales soumises aux BCR sont possibles sans qu'il soit nécessaire d'introduire une nouvelle demande d'autorisation, dans la mesure où les conditions suivantes sont remplies: |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| | | | | i) une personne désignée au sein du groupe actualise la liste des filiales, enregistre et consigne toute mise à jour des règles et fournit les informations requises aux personnes concernées ou aux autorités de protection des données, à leur demande;<br>ii) aucun transfert n'est effectué vers une nouvelle filiale tant que celle-ci n'est pas véritablement liée par les règles contraignantes et tant qu'elle n'est pas en mesure de les respecter;<br>iii) toute modification substantielle des règles ou de la liste des filiales doit être notifiée une fois par an aux autorités chargées de la protection des données délivrant les autorisations, assortie d'un bref exposé des motifs justifiant cette mise à jour. |
| **6 – GARANTIES CONCERNANT LA PROTECTION DES DONNÉES** | | | | |
| **6.1 Une description des principes de protection, y compris des règles en matière de transferts ou de transferts ultérieurs en dehors de l'UE.** | OUI | OUI | WP 108 point 8 (page 8) + WP 74 point 3.1, dernier § et point 3.2 (page 9) | Les BCR doivent expliquer comment les principes suivants sont respectés au sein de la société:<br>i) transparence, loyauté;<br>ii) limitation des finalités;<br>iii) qualité des données;<br>iv) sécurité, y compris l'obligation de passer des contrats avec tous les sous-traitants/responsables du traitement, précisant l'utilisation des données et les mesures de sécurité requises;<br>v) droits en matière d'accès, de rectification et d'opposition au traitement;<br>vi) limitations concernant les transferts et les transferts ultérieurs vers des sous-traitants et des responsables du traitement des données ne faisant pas partie du groupe (les membres du groupe responsables du traitement des données peuvent communiquer des données à des sous-traitants/responsables du traitement extérieurs au groupe et établis en dehors de l'UE, à condition qu'une protection adéquate soit assurée conformément aux articles 16, 17, 25 et 26 de la directive 95/46/CE). |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| **6.2 La liste des entités liées par les BCR** | NON | OUI | WP 108 point 7.1.3 (page 8) | Cf. également le point 5.1 du présent document; obligation faite à une personne ou à un département désigné(e) au sein du groupe de tenir une liste actualisée des entités liées par les BCR et nécessité d'informer les autorités de protection des données et les personnes concernées en cas de modification de la liste. |
| **6.3 Le besoin de transparence dans les cas où la législation nationale empêche le groupe d'observer les règles d'entreprise contraignantes** | OUI | NON | WP 74 point 3.3.3 (pages 13-14) | 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, ou tout autre délégué/instance chargé(e) de la confidentialité des données (à moins que cela ne soit interdit par une autorité chargée d'assurer le respect de la loi, par exemple une interdiction prévue par le code pénal pour préserver le secret de l'instruction).<br><br>En outre, un engagement doit être prévu, selon lequel, en cas de conflit entre la législation nationale et les obligations au titre des règles, le siège européen, la filiale européenne responsable par délégation de la protection des données ou tout autre délégué/instance chargé(e) de la confidentialité prendra une décision responsable sur l'action à entreprendre et, en cas de doute, consultera les autorités compétentes en matière de protection des données. |

| Critères pour l'approbation des BCR | Dans les BCR | Dans le formulaire de demande | Textes de référence | Commentaires |
|---|---|---|---|---|
| **6.4 Une déclaration concernant la relation entre la législation nationale et les règles d'entreprise contraignantes** | NON (pas requis, mais bienvenu) | NON (pas requis, mais bienvenu) | n/d | Bien que cela ne soit pas requis par les documents WP 74 et WP 108, il est très utile de préciser la relation qui existe entre les BCR et la législation applicable en la matière.<br><br>Les règles pourraient indiquer que, si la législation locale - par exemple, la législation communautaire - exige un niveau supérieur de protection des données personnelles, celle-ci prime sur les règles d'entreprise contraignantes.<br><br>Dans tous les cas, les données seront traitées conformément au droit applicable visé à l'article 4 de la directive 95/46/CE, ainsi qu'à la législation locale pertinente. |

Fait à Bruxelles, le 24.6.2008

*Pour le groupe de travail*
*Le Président*
*Alex TÜRK*