GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

00658/13/FR
WP 204

Document explicatif sur les règles d'entreprise contraignantes applicables aux sous-traitants

Adopté le 19 avril 2013

Ce 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 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice de la Commission européenne, B-1049 Bruxelles, Belgique, bureau n° MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/article-29/index_fr.htm

TABLE DES MATIÈRES

page

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1],

vu les articles 29 et 30, paragraphe 1, point a), et paragraphe 3, de ladite directive,

vu son règlement intérieur et, en particulier, ses articles 12 et 14,

a adopté le présent document de travail:

1. CONTEXTE

1.1. Règles de l'Union européenne pour les transferts internationaux de données

La directive requiert d'encadrer strictement les transferts de données vers les pays tiers afin de garantir que les personnes concernées bénéficient d'un niveau de protection adéquat même lorsque leurs données sont envoyées en dehors de l'Union européenne (ci-après «l'UE»).

L'article 26, paragraphe 2, de la directive prévoit que *«[…] un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat […], lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées*».

Par conséquent, lorsque le pays de l'importateur de données n'assure pas un niveau de protection adéquat, le responsable du traitement doit offrir des garanties suffisantes concernant les données transférées, par exemple par l'adoption de clauses contractuelles.

Compte tenu de ce qui précède, et afin de favoriser le respect de la directive 95/46/CE concernant les transferts de données vers un pays tiers, la Commission européenne a adopté des séries de clauses contractuelles types pour encadrer les transferts entre responsables du traitement (2001/497/CE du 15 juin 2001, et 2004/915/CE du 27 décembre 2004) et les transferts entre les responsables du traitement et les sous-traitants (2010/87/UE du 5 février 2010).

1.2. Règles d'entreprise contraignantes applicables aux responsables du traitement

Étant donné que les organisations doivent avoir une approche globale de la protection des données, le groupe de travail «article 29» a estimé nécessaire de les autoriser à adopter des règles internes contraignantes, appelées «règles d'entreprise contraignantes» (ci-après «BCR»), en vue de réglementer les transferts de données à caractère personnel qui sont initialement traitées par l'organisation, en tant que responsable du traitement, au sein de la

[1] Journal officiel L 281 du 23.11.1995, p. 31, disponible à l'adresse suivante: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML.

même organisation. Les autorités européennes chargées de la protection des données ont créé une «boîte à outils» décrivant les éléments que devraient contenir les BCR[2].

Il importe de noter par ailleurs que, si les clauses contractuelles types sont une solution «prête à l'emploi», chaque série de BCR doit, elle, être adaptée en fonction des besoins particuliers d'une entreprise donnée. En outre, alors que les clauses contractuelles types sont généralement signées sans nécessité d'une mise en œuvre particulière, les BCR supposent que l'organisation dispose déjà, au sein du groupe, d'un régime de protection des données suffisamment solide et satisfaisant ou qu'elle mette en place les mesures nécessaires pour que les systèmes existants répondent aux exigences des BCR.

Au cours des dernières années, le succès des BCR applicables aux responsables du traitement n'a cessé de croître. La longueur de la procédure d'adoption a été considérablement réduite, non seulement grâce à la plus grande expérience des organisations et des autorités chargées de la protection des données mais aussi à la procédure de reconnaissance mutuelle. De plus, les organisations multinationales ont constamment réaffirmé que les BCR s'inscrivent dans l'approche pragmatique qu'elles recherchent à l'égard des questions de conformité. En outre, la Commission européenne a apporté son soutien aux BCR en les intégrant à la proposition de règlement sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, publiée le 25 janvier 2012[3].

1.3. Règles d'entreprise contraignantes applicables aux sous-traitants

En 2010, la Commission européenne a adopté une nouvelle série de clauses contractuelles types pour les transferts de données entre les responsables du traitement et les sous-traitants, afin de répondre à l'expansion des activités de traitement et, en particulier, à l'apparition de nouveaux modèles de gestion pour le traitement international des données à caractère personnel. Ces clauses contractuelles types de 2010 contiennent des dispositions spécifiques autorisant, dans certaines conditions, l'externalisation des activités de traitement vers des sous-traitants ultérieurs, tout en offrant des garanties suffisantes concernant les données personnelles transférées.

Garantir en permanence un niveau de protection adéquat grâce aux outils créés pour encadrer les transferts internationaux de données, ainsi qu'il est décrit plus haut, se révèle difficile, principalement à cause de la complexité et du nombre croissants de transferts internationaux de données (résultant, par exemple, de l'informatique en nuage, de la mondialisation, des centres de données, des réseaux sociaux, etc.).

Si les clauses contractuelles types semblent suffire pour encadrer les transferts non massifs effectués par un exportateur de données établi dans l'UE vers un importateur de données établi dans un pays tiers, les professionnels de la sous-traitance, eux, demandent depuis longtemps un nouvel instrument juridique qui permette une approche globale de la protection des données dans le milieu de la sous-traitance et qui reconnaisse officiellement les règles internes que les organisations peuvent avoir mises en œuvre. Ce nouvel instrument juridique permettrait d'encadrer les transferts massifs effectués par un sous-traitant vers des

---

[2] Voir les documents de travail WP153, WP154 et WP155, disponibles en anglais à l'adresse suivante: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm.

[3] Voir l'article 42 de la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf.

sous-traitants ultérieurs appartenant à la même organisation et agissant pour le compte d'un responsable du traitement, selon ses instructions. Vu l'intérêt croissant que portait l'industrie à un tel instrument, le groupe de travail a adopté, en 2012, un document de travail qui établissait un tableau présentant les éléments et principes que doivent contenir les règles d'entreprise contraignantes applicables aux sous-traitants[4] et un formulaire de demande d'approbation de ces règles[5]. Le groupe de travail a confirmé le lancement des règles d'entreprise contraignantes applicables aux sous-traitants le 5 décembre 2012[6].

2. DÉFINITION ET QUESTIONS JURIDIQUES EN JEU

2.1. Portée de cet instrument et définitions

Les BCR applicables aux sous-traitants visent à faciliter la définition d'un cadre pour les transferts internationaux de données à caractère personnel qui sont initialement traitées par un sous-traitant pour le compte d'un responsable européen du traitement des données et selon ses instructions[7], et qui sont traitées ultérieurement au sein de l'organisation du sous-traitant.

En conséquence, les BCR applicables aux sous-traitants doivent être annexées au contrat conclu avec le sous-traitant (désigné, dans le présent document, sous le nom d'«accord de niveau de service» ou de «contrat de service») qu'impose l'article 17 de la directive 95/46/CE et qui contient notamment les instructions du responsable du traitement convenues entre le responsable du traitement externe et le sous-traitant. Ces BCR doivent être considérées comme des garanties suffisantes apportées par ce dernier au responsable du traitement (article 26, paragraphe 2, de la directive 95/46/CE) permettant à celui-ci de se conformer à la législation de l'UE en vigueur en matière de protection des données. Les entités du groupe du sous-traitant doivent s'engager à respecter les principes contenus dans les BCR applicables aux sous-traitants et être responsables vis-à-vis du responsable du traitement en cas d'infraction auxdites BCR.

Il importe toutefois d'insister sur le fait que, même si les autorités européennes chargées de la protection des données examinent le contenu des BCR applicables aux sous-traitants du groupe d'un sous-traitant afin de vérifier que toutes les exigences énoncées dans le document WP195 sont satisfaites, le responsable du traitement reste chargé de veiller à ce que des garanties suffisantes soient offertes en ce qui concerne les données transférées et traitées pour son compte et selon ses instructions au sein des entités du groupe du sous-traitant.

Le groupe de travail rappelle que les BCR applicables aux sous-traitants ne visent pas à déplacer les obligations des responsables du traitement vers les sous-traitants. Les obligations respectives des uns et des autres dans le cadre des transferts internationaux de données demeureront inchangées (à l'instar des clauses contractuelles types édictées par la

---

4 Voir le document de travail WP195, adopté le 6 juin 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_fr.pdf.

5 Voir le formulaire de demande d'approbation des règles d'entreprise contraignantes applicables au transfert des données à caractère personnel pour les activités de traitement, adopté le 17 septembre 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_application_form_en.doc (en anglais).

6 Voir le communiqué de presse du 21 décembre 2012, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf (en anglais).

7 Un responsable du traitement dans un pays tiers a demandé à une entreprise de sous-traitance d'effectuer des transferts internationaux de ces données à des entités de son groupe d'entreprises en qualité de sous-traitants ultérieurs.

directive 2010/87/UE) mais certains outils devront être adaptés aux spécificités des transferts au sein d'un même groupe d'organisations (un engagement général au lieu de plusieurs contrats) et aux spécificités des BCR (outils de responsabilisation tels qu'audits, programmes de formation, délégués à la protection des données, etc.).

En outre, les BCR applicables aux sous-traitants doivent renforcer les droits des personnes concernées en prévoyant expressément que les sous-traitants s'engagent à fournir aux responsables du traitement les informations pertinentes pour leur permettre de s'acquitter de leurs obligations à l'égard des personnes concernées. Les BCR applicables aux sous-traitants apparaissent ainsi comme une garantie supplémentaire que les sous-traitants fourniront les informations pertinentes aux responsables du traitement.

Enfin, le fait qu'un sous-traitant doive demander à l'UE de reconnaître que ses BCR applicables aux sous-traitants constituent des garanties appropriées pour les transferts internationaux au titre des procédures de coopération et de reconnaissance mutuelle prévues dans le document de travail WP107[8] ne dispensera pas les responsables du traitement de l'obligation d'obtenir une autorisation nationale des autorités compétentes chargées de la protection des données pour transférer des données aux différentes entités de leurs prestataires de services (sous-traitants, sous-traitants ultérieurs, centres de données, etc.), étant donné que les BCR applicables aux sous-traitants font partie des garanties offertes par les responsables du traitement.

2.2. Transferts et transferts ultérieurs

2.2.1. Transferts au sein du groupe du sous-traitant

Puisque, aux termes du document de travail WP195, les données ne peuvent faire l'objet d'un traitement ultérieur par d'autres filiales du groupe du sous-traitant qu'à condition que le responsable du traitement[9] en ait été préalablement informé et qu'il y ait donné son consentement écrit préalable, les BCR applicables aux sous-traitants assurent une transparence à l'égard du responsable du traitement et laissent à ce dernier le contrôle des données traitées, pour son compte et selon ses instructions, par les entités du groupe du sous-traitant.

Les parties au contrat de service sont libres de décider, en fonction de leurs besoins particuliers, s'il suffit que le responsable du traitement marque son consentement général préalable au début du service ou s'il doit donner un consentement spécifique pour chaque nouveau traitement ultérieur. Si un consentement général est accordé, toute modification prévue concernant l'ajout ou le remplacement d'un sous-traitant doit être notifiée au responsable du traitement en temps opportun afin de lui permettre de s'y opposer ou de résilier le contrat avant que les données ne soient communiquées au nouveau sous-traitant ultérieur.

L'organisation d'un sous-traitant liée par des BCR applicables aux sous-traitants ne sera pas tenue de signer de contrat, pour encadrer les transferts, avec chaque sous-traitant ultérieur qui

[8] Voir le document de travail WP107, adopté le 14 avril 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_fr.pdf#h2-2.

[9] Les informations à fournir au responsable du traitement concernent les principaux éléments (parties concernées, pays, sécurité, garanties en cas de transferts internationaux et, si besoin est, copie des contrats utilisés). Des informations plus détaillées (comme le nom des sous-traitants ultérieurs) pourront aussi être fournies, par exemple, dans un registre numérique accessible au public.

fait partie de son organisation, puisque ces BCR offrent des garanties concernant les données transférées et traitées pour le compte d'un responsable du traitement et selon ses instructions.

2.2.2. Transferts ultérieurs vers des sous-traitants ultérieurs externes

En plus des règles énoncées ci-dessus pour les transferts au sein du groupe du sous-traitant (transparence, consentement du responsable du traitement), une filiale du groupe du sous-traitant ne peut déléguer les obligations qui lui incombent en vertu du contrat de service (article 17 de la directive) à un sous-traitant ultérieur externe (en dehors du groupe) que par voie de contrat conclu par écrit avec ce dernier, stipulant qu'une protection adéquate est assurée conformément aux articles 16 et 17 de la directive 95/46/CE et précisant que le sous-traitant ultérieur externe est tenu de respecter les mêmes obligations que celles imposées à la filiale du groupe soumise aux BCR en vertu du contrat de service et des points 1.3, 1.4, 3 et 6 du document de travail 195[10]. En outre, dans la mesure où les BCR applicables aux sous-traitants ne s'appliquent pas aux transferts vers des sous-traitants ultérieurs externes (en dehors du groupe), une protection adéquate doit être assurée pour ces transferts conformément aux articles 25 et 26 de la directive 95/46/CE.

2.3. Considérations concernant le caractère contraignant des BCR applicables aux sous-traitants

Les sous-traitants répondent aux besoins créés par leurs activités de traitement de données en fonction de différents contextes juridiques et culturels et de différentes philosophies et pratiques professionnelles. Il ressort clairement de l'expérience acquise avec les BCR applicables aux responsables du traitement que presque toutes les organisations multinationales ont une approche différente de la question. Néanmoins, il est notamment un élément important qui doit figurer dans tous les systèmes si ces derniers servent à apporter des garanties concernant les transferts de données vers les pays tiers pour des activités de traitement: le caractère contraignant des règles d'entreprise applicables aux sous-traitants, tant au niveau interne qu'à l'égard du monde extérieur (opposabilité des règles).

2.3.1. Caractère contraignant des règles d'entreprise applicables aux sous-traitants au sein de l'organisation[11]

On peut établir une distinction entre le problème du respect des règles et celui de leur opposabilité juridique.

En effet, l'évaluation du «caractère contraignant» de ces règles d'entreprise applicables aux sous-traitants emporte une évaluation commune de leur caractère contraignant en interne et en externe dans la législation.

À cet égard, le caractère contraignant des règles en interne implique que les filiales de l'organisation du sous-traitant, ainsi que ses employés, sont tenus de respecter les règles internes. Sur ce point, des éléments pertinents pourraient être, notamment, l'existence de sanctions disciplinaires en cas d'infraction aux règles, l'information individuelle et effective des employés, la mise en place de programmes de formation spéciaux pour les employés et les sous-traitants, etc. Tous ces éléments, également examinés à la section 4, pourraient expliquer

[10] *Op. cit*. 6.

[11] Les entreprises sont fréquemment réticentes à adopter un code de conduite car cela comporte des risques élevés, voire des conséquences juridiques, pour les organisations qui ne respectent pas leur propre code.

pourquoi les personnes faisant partie de l'organisation du sous-traitant se sentent obligées de respecter ces règles.

En ce qui concerne les filiales du groupe du sous-traitant, il n'appartient pas au groupe de travail de déterminer la manière dont les organisations doivent garantir que toutes les filiales sont effectivement liées par les règles ou se sentent obligées de les respecter, même s'il existe des exemples bien connus, comme les codes de conduite internes qui s'appuient sur des accords intragroupe[12]. Toutefois, les organisations doivent garder à l'esprit que si elles demandent l'approbation de leurs BCR applicables aux sous-traitants en tant que garanties appropriées offertes par le sous-traitant au responsable du traitement (article 26, paragraphe 2, de la directive 95/46/CE), elles doivent démontrer aux autorités de protection des données que ces BCR sont en effet contraignantes dans tout le groupe.

Le caractère contraignant en interne des règles doit être manifeste et suffisamment élevé pour pouvoir garantir le respect des règles en dehors de l'UE, normalement sous la responsabilité du siège européen du sous-traitant, de la filiale européenne chargée, par délégation, d'assurer la protection des données, ou du sous-traitant européen exportateur de données, qui doivent prendre toutes les mesures nécessaires pour garantir que les filiales adaptent leurs activités de traitement ultérieur aux engagements figurant dans les BCR[13].

En réalité, dans la plupart des cas, une filière de l'organisation, établie dans l'UE, offre des garanties suffisantes et s'occupe de la demande du sous-traitant concernant les BCR auprès de la principale autorité chargée de la protection des données. Si l'organisation a son siège en dehors de l'UE, elle devrait déléguer ces responsabilités à une filiale établie dans l'UE, s'il en existe. Il est logique que celui qui offre les garanties reste responsable du respect effectif des règles et de l'application des garanties. Toutefois, un autre mécanisme peut être accepté: que la responsabilité incombe au sous-traitant européen exportateur des données. Voir à ce sujet les sections 4.6 et 4.7 sur la responsabilité et la juridiction.

2.3.2. Caractère contraignant des règles d'entreprise applicables aux sous-traitants pour les sous-traitants ultérieurs externes qui traitent les données

Si le sous-traitant délègue les obligations qui lui incombent en vertu du contrat de service (article 17 de la directive) à un sous-traitant ultérieur externe, avec le consentement du responsable du traitement, il ne doit le faire que par voie de contrat écrit conclu avec le sous-traitant ultérieur. Voir à ce sujet la section 2.2.2 sur les transferts ultérieurs.

2.3.3. Opposabilité juridique des règles d'entreprise

2.3.3.1. Opposabilité des règles d'entreprise par les personnes concernées (droits de tiers bénéficiaires)

Les personnes concernées relevant du champ d'application des BCR applicables aux sous-traitants doivent devenir des tiers bénéficiaires par l'inclusion d'une clause de tiers bénéficiaire dans les BCR, qui doit être rendue contraignante soit par des engagements

[12] Il y a lieu de noter que, dans certains États membres, seuls les contrats sont considérés comme contraignants. Il est dès lors recommandé de se faire conseiller au niveau local si le recours à d'autres instruments juridiques que les contrats est envisagé.

[13] En vertu du droit international des sociétés, les filiales peuvent s'opposer des codes de conduite les unes aux autres en invoquant une violation quasi-contractuelle, une fausse déclaration ou une faute.

unilatéraux (si possible en vertu de la législation nationale) ou par des accords contractuels entre les filiales du groupe du sous-traitant.

Quoi qu'il en soit, les personnes concernées peuvent contraindre le responsable du traitement à respecter les règles d'entreprise en déposant plainte auprès des autorités de protection des données ou du tribunal compétent à l'égard du responsable européen du traitement, tel qu'il est expliqué à la section 4.6.

Toutefois, si les personnes concernées ne sont pas en mesure d'introduire une plainte contre le responsable du traitement[14], elles peuvent également intenter des poursuites contre le sous-traitant auprès des autorités chargées de la protection des données ou du tribunal compétent à l'égard i) du siège européen du sous-traitant, ou ii) de sa filiale européenne responsable par délégation de la protection des données, ou iii) du sous-traitant européen exportateur de données.

Si cela se révèle impossible (par exemple, si le sous-traitant n'a pas de filiale dans l'UE), les personnes concernées ont le droit de déposer plainte auprès du tribunal de leur lieu de résidence. En tout état de cause, si la législation nationale prévoit des solutions plus favorables pour la personne concernée (par exemple, le droit du travail ou le droit de la consommation), celles-ci s'appliqueront.

Si, dans certains cas, l'opposabilité juridique d'une clause de tiers bénéficiaire contenue dans des déclarations unilatérales est incontestable, dans d'autres États membres, la situation est moins claire et il se peut que des déclarations unilatérales ne suffisent pas en soi. Lorsque de telles déclarations ne peuvent être considérées comme octroyant des droits de tiers bénéficiaire opposables, les organisations devront mettre en place les accords contractuels nécessaires à cet effet. Les accords contractuels sont légalement opposables en vertu du droit privé dans tous les États membres[15].

Les principes couverts par les BCR qui doivent être rendus opposables par la clause de tiers bénéficiaire sont les suivants:

- l'obligation pour le sous-traitant de respecter les BCR ainsi que les instructions du responsable du traitement relatives au traitement des données et aux mesures de sécurité et de confidentialité, telles qu'énoncées dans le contrat de service (WP195, section 1.1);

- la création de droits de tiers bénéficiaires pour les personnes concernées (WP195, section 1.3);

- la responsabilité du sous-traitant de verser une éventuelle indemnisation et de remédier aux infractions aux BCR (WP195, section 1.5);

- la charge de la preuve incombant au sous-traitant, et non à la personne concernée (WP195, section 1.7);

---

[14] Cela peut être le cas si le responsable du traitement a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, à moins que l'ensemble de ses obligations juridiques n'ait été transféré, par contrat ou par l'effet de la loi, au successeur légal, contre lequel la personne concernée peut alors faire valoir ses droits.

[15] À l'heure actuelle, il est possible d'accorder des droits de tiers bénéficiaire dans tous les États membres. Voir les expériences antérieures avec les clauses contractuelles types et les tiers bénéficiaires.

- l'accès aisé des personnes concernées aux BCR (WP195, section 1.8);

- l'existence d'un processus de traitement des plaintes concernant les BCR (WP195, section 2.2);

- une obligation de coopérer avec les autorités de protection des données (WP195, section 3.1) et avec le responsable du traitement (WP195, section 3.2);

- les principes de protection de la vie privée (WP195, section 6.1);

- la liste des entités liées par les BCR (WP195, section 6.2);

- une transparence dans les cas où la législation nationale empêche le sous-traitant d'observer les BCR (WP195, section 6.3).

Les accords contractuels ne doivent pas nécessairement être complexes ou longs. Ils ne sont que des instruments destinés à faire naître des droits de tiers bénéficiaires en faveur des personnes se trouvant dans les pays où il n'est pas assuré que des déclarations unilatérales puissent produire un résultat similaire. Dans certains cas, il peut suffire d'ajouter une simple clause à d'autres contrats en place entre les filiales du groupe du sous-traitant.

2.3.3.2. Opposabilité des règles d'entreprise par le responsable du traitement

Les BCR applicables aux sous-traitants constituent une garantie concernant les transferts internationaux offerte par un sous-traitant à son client (le responsable du traitement) et c'est le responsable du traitement qui assume en premier lieu, vis-à-vis des autorités de protection des données et des personnes concernées, la responsabilité de la protection des données à caractère personnel transférées en dehors de l'UE. À ce titre, les BCR applicables aux sous-traitants doivent être rendues contraignantes pour le responsable du traitement grâce à l'introduction d'une référence explicite à ces règles dans le contrat de service.

En plus des éléments cités ci-dessus, et afin que les BCR applicables aux sous-traitants soient liées, sans ambiguïté aucune, à l'accord de niveau de service (ci-après «ANS») signé avec chaque client (responsable du traitement), il importe de s'assurer que les dispositions de l'ANS incluent les éléments et engagements suivants:

- le responsable du traitement s'engage, en cas de transfert concernant des catégories spéciales de données, à s'assurer que la personne concernée a été ou sera informée, avant le transfert, du fait que ses données pourraient être transmises à un pays tiers ne garantissant pas une protection adéquate;

- le responsable du traitement s'engage, en outre, à informer la personne concernée de l'existence des BCR et de sous-traitants établis hors de l'Union européenne. Sur demande, le responsable du traitement mettra à disposition des personnes concernées une copie des BCR et de l'ANS (exempte de toutes informations commerciales sensibles et confidentielles);

- l'ANS décrit clairement les mesures de confidentialité et de sécurité à respecter ou il y fait référence au moyen d'un lien électronique;

- l'ANS décrit clairement les instructions et le traitement des données;

- l'ANS précise si les données peuvent être sous-traitées au sein du groupe ou en dehors du groupe, et si le consentement préalable du responsable du traitement est général ou doit être donné pour chaque nouvelle activité de sous-traitance.

Les autorités de protection des données qui examinent les BCR ne demanderont pas forcément de produire ce contrat de service mais, dans tous les cas, un résumé étayé par des extraits de cet accord sera joint au formulaire de demande afin d'expliquer la manière dont les BCR applicables aux sous-traitants sont rendues opposables en faveur des responsables du traitement.

En outre, les BCR incluront une clause de droits de tiers bénéficiaire en faveur du responsable du traitement, afin de lui garantir le droit d'opposer les BCR à toutes les filiales du groupe du sous-traitant, clause qui couvrira le droit de recours juridictionnel ainsi que le droit à réparation.

2.3.3.3. Opposabilité des règles d'entreprise par les autorités de protection des données

Si un sous-traitant demande à l'UE de reconnaître ses BCR applicables aux sous-traitants en tant que garanties appropriées offertes par le sous-traitant au responsable du traitement (article 26, paragraphe 2, de la directive 95/46/CE), il est évident que le groupe du sous-traitant s'engage à l'égard des autorités européennes chargées de la protection des données à respecter les garanties offertes (dans le cas présent, les BCR applicables aux sous-traitants). Il incombe néanmoins au responsable du traitement de demander l'autorisation nationale obligatoire pour le transfert international de données, qui doit être clairement distinguée de la reconnaissance des BCR en tant que garanties suffisantes concernant les transferts de données. Les BCR applicables aux sous-traitants déjà «approuvées» (et non «autorisées») à l'échelle européenne seront mentionnées par le responsable du traitement au titre des garanties appropriées offertes pour les transferts internationaux.

Dans la mesure où l'article 28 de la directive 95/46/CE prévoit que les autorités de protection des données *«(...) sont chargées de surveiller l'application, sur [leur] territoire, des dispositions adoptées par les États membres en application de la présente directive*», cela signifie qu'elles ont l'obligation, entre autres, de superviser les transferts et d'évaluer les garanties offertes pour les transferts de données en dehors de l'UE.

Afin de s'acquitter de ces missions, les autorités de protection des données sont investies de pouvoirs d'enquête, de pouvoirs effectifs d'intervention sur leur territoire ainsi que du pouvoir d'entamer des poursuites judiciaires, ces pouvoirs pouvant être utilisés à l'encontre d'un sous-traitant qui ne respecte pas les BCR.

En outre, une infraction aux BCR applicables aux sous-traitants commise par une filiale du groupe du sous-traitant (ou par l'ensemble du groupe) pourrait conduire au retrait de l'autorisation du transfert concerné accordée au responsable du traitement sur la base des BCR applicables aux sous-traitants. Ce retrait ne serait pas rétroactif.

2.3.4. Exigences imposées par le droit national et applicables aux filiales de l'organisation

Les BCR doivent clairement mentionner que, lorsqu'une filiale du groupe soumise aux BCR a des raisons de penser que la législation actuelle ou future qui lui est applicable risque de l'empêcher de se conformer aux instructions reçues du responsable du traitement des données

ou de remplir les obligations qui lui incombent en vertu des BCR ou du contrat de service, elle doit en informer sans délai:

- le responsable du traitement, qui peut suspendre le transfert des données et/ou résilier le contrat;

- le siège européen du sous-traitant, la filiale européenne responsable par délégation de la protection des données ou tout autre délégué/instance chargé(e) de la confidentialité des données chez le sous-traitant; et

- l'autorité de protection des données dont relève le responsable du traitement.

En outre, le sous-traitant communique sans délai au responsable du traitement toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité répressive, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière. Dans tous les cas, la demande de divulgation sera mise en attente et l'autorité de protection des données dont relève le responsable du traitement ainsi que l'autorité chef de file pour les BCR en seront expressément informées.

Il conviendra toutefois de veiller à ce que les transferts de données à caractère personnel à une autorité répressive reposent sur des motifs légaux en vertu du droit applicable, dans la mesure où les exigences concernant les BCR applicables aux sous-traitants, énoncées à la section 6.3 du document de travail WP195, ne créent qu'une procédure d'information (voir ci-dessus) qui ne légitime pas les transferts en soi. En cas de lois contradictoires, il sera renvoyé aux traités et accords internationaux applicables en la matière.

3. CONTENU MATÉRIEL DES RÈGLES D'ENTREPRISE CONTRAIGNANTES APPLICABLES AUX SOUS-TRAITANTS

3.1. Contenu matériel et niveau de détail

Les principes de protection des données de la directive doivent être développés et détaillés dans les BCR applicables aux sous-traitants afin que ces dernières soient adaptées, de manière pratique et réaliste, aux activités de traitement réalisées par l'organisation dans les pays tiers et qu'elles puissent être comprises et bien appliquées par les organes chargés de la protection des données au sein de l'organisation.

La section 6 du document de travail WP195 fournit de plus amples explications sur ce contenu.

La description des transferts ne peut être que générale dans les BCR, mais des informations plus précises sur les transferts particuliers d'un responsable du traitement déterminé devront être fournies dans le cadre de la procédure d'autorisation nationale engagée auprès des autorités compétentes chargées de la protection des données. Le niveau de détail dans les BCR doit être suffisant pour permettre à ces autorités d'évaluer le caractère adéquat des garanties offertes concernant le traitement et le traitement ultérieur des données réalisés dans les pays tiers par une filiale du groupe du sous-traitant.

3.2. Actualisations des BCR

Le groupe de travail «article 29» reconnaît que les organisations sont des entités en mutation dont les filiales et les pratiques sont susceptibles de changer fréquemment, de sorte que les transferts qui ont lieu pour le compte du responsable du traitement et selon ses instructions et, bien entendu, les règles contenues dans les BCR ne peuvent pas correspondre en permanence à la réalité au moment où la protection adéquate est reconnue.

Partant, les BCR applicables aux sous-traitants peuvent être modifiées (par exemple, pour tenir compte des 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, aux autorités chargées de la protection des données et au responsable du traitement.

En cas de modification ayant une incidence sur les conditions de traitement, celle-ci doit être notifiée au responsable du traitement en temps utile pour lui permettre de s'y opposer ou de résilier le contrat avant que la modification ne soit effectuée (à titre d'exemple, toute modification prévue concernant l'ajout ou le remplacement d'un sous-traitant doit être notifiée avant que les données ne soient communiquées au nouveau sous-traitant).

Les BCR applicables aux sous-traitants et la liste des filiales qui y sont soumises peuvent être actualisées sans qu'il soit nécessaire d'introduire une nouvelle demande d'autorisation, dans la mesure où les conditions suivantes sont remplies:

i) une personne désignée tient à jour la liste des filiales du groupe et des sous-traitants ultérieurs participant aux activités de traitement des données pour le responsable du traitement, et cette liste est mise à la disposition de ce dernier, des personnes concernées et des autorités de protection des données;

ii) la personne susmentionnée enregistre et consigne toutes les mises à jour des règles et fournit systématiquement les informations requises au responsable du traitement et aux autorités chargées de la protection des données sur demande;

iii) aucun transfert n'est effectué vers une nouvelle filiale tant que celle-ci n'est pas effectivement liée par les BCR applicables aux sous-traitants et qu'elle n'est pas en mesure de les respecter;

iv) toute modification substantielle des BCR applicables aux sous-traitants ou de la liste des filiales doit être notifiée une fois par an aux autorités chargées de la protection des données qui délivrent les autorisations, assortie d'un bref exposé des motifs justifiant cette mise à jour.

L'actualisation des règles doit s'inscrire dans un contexte où les procédures de travail sont susceptibles de changer et où les règles doivent être adaptées à ces environnements en mutation.

4. ASSURER LE RESPECT ET GARANTIR L'EXÉCUTION

Outre les règles traitant des principes de fond de la protection des données, toute règle d'entreprise contraignante applicables aux sous-traitants doit également contenir les éléments suivants:

4.1. Dispositions garantissant un niveau de respect acceptable

Les règles doivent mettre en place un système qui garantit la connaissance et l'application des règles au sein et en dehors de l'Union européenne. La publication par le siège du groupe de politiques internes de protection de la vie privée ne saurait être considérée que comme une première mesure du processus visant à apporter des garanties suffisantes au sens de l'article 26, paragraphe 2, de la directive. L'organisation demandeuse doit également être en mesure de prouver que cette politique est connue, comprise et effectivement appliquée dans tout le groupe par les employés qui ont reçu une formation appropriée et ont accès en permanence aux informations pertinentes (y compris les BCR), par exemple via l'intranet. L'organisation devrait désigner, avec l'aide de la direction, le personnel qualifié chargé de surveiller et de garantir le respect des règles.

4.2. Audits

Les règles doivent prévoir, à intervalles réguliers, des audits en matière de protection des données et/ou une supervision externe par des contrôleurs internes ou externes agréés, dont le résultat sera directement communiqué au délégué ou à l'instance chargé(e) de la protection des données ainsi qu'au conseil d'administration de la société-mère du groupe, et sera rendu accessible, sur demande, au responsable du traitement[16].

Les BCR doivent également mentionner que les autorités chargées de la protection des données dont relève le responsable du traitement des données peuvent avoir accès, sur demande, aux résultats de l'audit et qu'elles sont habilitées à réaliser elles-mêmes des audits sur la protection des données, si ceux-ci se révèlent nécessaires et possibles sur le plan juridique. Ce cas est le plus susceptible de se produire lorsque les audits prévus au paragraphe précédent ne sont pas disponibles, pour quelque raison que ce soit, lorsque les audits ne contiennent pas les informations pertinentes nécessaires à un suivi normal de l'approbation délivrée par les autorités de protection des données ou lorsque l'urgence de la situation plaide en faveur d'une participation directe des autorités de protection des données dont relève le responsable du traitement concerné.

Ces audits se déroulent conformément aux lois et règlements en vigueur régissant les pouvoirs d'enquête des autorités de protection des données, sans préjudice des pouvoirs d'inspection de chaque autorité de protection des données. En tout état de cause, ils ont lieu dans le plein respect de la confidentialité et des secrets commerciaux et se limitent étroitement à la vérification du respect des règles d'entreprise contraignantes.

En outre, les BCR applicables aux sous-traitants doivent mentionner que tout sous-traitant ou sous-traitant ultérieur chargé de gérer les données d'un responsable du traitement particulier

[16] Le contenu de ces audits doit être complet et approfondir, en tout cas, certains détails déjà mentionnés dans le présent document de travail, comme l'existence de transferts ultérieurs sur la base de clauses contractuelles types (voir section 2.2.2) ou les décisions prises au sujet d'exigences imposées par le droit national qui risquent d'entrer en conflit avec les règles d'entreprise contraignantes (voir section 3.3.3).

accepte de soumettre, à la demande de ce dernier, ses installations de traitement des données à une vérification des activités de traitement relatives audit responsable; cette vérification sera effectuée par le responsable du traitement lui-même ou par un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, soumis à une obligation de confidentialité et choisis par le responsable du traitement, s'il y a lieu, avec l'accord de l'autorité chargée de la protection des données.

Le formulaire de demande inclura une description du système d'audit, précisant par exemple:

- l'entité (département au sein du groupe) qui décide du plan/programme d'audit,
- l'entité qui mènera l'audit,
- la fréquence de l'audit (régulièrement ou sur demande spécifique du responsable de la protection des données),
- le champ couvert par l'audit [à titre d'exemple, les applications, systèmes informatiques, bases de données gérant des données à caractère personnel, ou les transferts ultérieurs, les décisions prises au sujet d'une exigence imposée par le droit national qui est contraire aux BCR applicables aux sous-traitants, le réexamen des clauses contractuelles appliquées aux transferts en dehors du groupe (vers les responsables du traitement des données ou les sous-traitants), les actions correctives, etc.],
- l'entité qui recevra les résultats des audits.

4.3. Traitement des plaintes

Les BCR applicables aux sous-traitants doivent mentionner que le groupe du sous-traitant s'engage à créer un point de contact spécifique à l'intention des personnes concernées.

Toutes les filiales soumises à ces BCR sont uniquement tenues de transmettre sans délai les plaintes et demandes au responsable du traitement, sans obligation de les traiter (sauf disposition contraire convenue avec le responsable du traitement).

Ce n'est que lorsque le responsable du traitement des données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable que le sous-traitant est tenu de traiter ces communications.

Dans les cas où le sous-traitant assure le traitement des plaintes (lorsque c'est convenu avec le responsable du traitement ou que ce dernier a matériellement disparu ou a cessé d'exister), le département ou la personne chargé(e) de les traiter doit être clairement identifié et jouir d'un degré adéquat d'indépendance dans l'exercice de ses fonctions.

En pareils cas, il convient de fournir aux personnes concernées les informations suivantes:

- où déposer plainte,
- sous quelle forme,
- le délai de réponse à la plainte,
- les conséquences en cas de rejet de la plainte,

- les conséquences si la plainte est jugée recevable,

- les conséquences si la personne concernée n'est pas satisfaite des réponses (droit d'introduire un recours devant le tribunal/l'autorité chargée de la protection des données).

4.4. L'obligation de coopérer avec le responsable du traitement

Les BCR applicables aux sous-traitants doivent mentionner expressément que les filiales et les employés du groupe ont l'obligation de respecter les instructions relatives au traitement des données et aux mesures de sécurité et de confidentialité, telles qu'énoncées dans le contrat de service (article 17 de la directive).

Les règles doivent clairement indiquer l'obligation, pour tout sous-traitant ou sous-traitant ultérieur, de coopérer avec le responsable du traitement et de l'aider à se conformer à la législation relative à la protection des données (laquelle prévoit, entre autres, l'obligation de respecter les droits des personnes concernées et de traiter leurs plaintes, ou celle d'être en mesure de répondre aux enquêtes ou aux demandes émanant de l'autorité de protection des données). Cette obligation de coopération et d'assistance est exécutée dans un délai raisonnable et autant que faire se peut.

4.5. L'obligation de coopérer avec les autorités de protection des données

Comme l'énonce le document de travail WP12, l'un des éléments les plus importants pour évaluer l'adéquation d'un système d'autorégulation est le niveau d'assistance et de soutien dont disposent les 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, en effet, d'un élément important des BCR applicables aux sous-traitants: les règles doivent clairement mentionner l'obligation, pour toutes les filiales du groupe du sous-traitant, de coopérer avec les autorités de protection des données dont relève le responsable du traitement concerné, de sorte que les personnes physiques puissent bénéficier du soutien institutionnel mentionné dans le document de travail WP12.

Doit également figurer un engagement non équivoque déclarant que l'organisation dans son ensemble et chacune de ses filiales séparément suivront les conseils des autorités compétentes chargées de la protection des données sur toute question liée à l'interprétation et l'application de ces BCR applicables aux sous-traitants.

Avant d'émettre des conseils, les autorités compétentes chargées de la protection des données peuvent demander l'avis de l'organisation, des personnes concernées, du responsable du traitement concerné et des autorités de protection des données qui peuvent être associées à la suite de la procédure coordonnée prévue dans le présent document de travail[17]. Les conseils peuvent être rendus publics.

En plus de toute disposition pertinente au niveau national, un refus grave et/ou persistant de l'organisation de coopérer ou de suivre les conseils des autorités compétentes chargées de la protection des données peut entraîner la suspension ou le retrait de l'autorisation de transfert

[17] Voir chapitre 5.

accordée au(x) responsable(s)s du traitement concerné(s), soit par les autorités de protection des données elles-mêmes, soit par l'autorité compétente en vertu du droit national habilitée pour ce faire. Une conséquence directe de ladite suspension ou dudit retrait obligera le(s) responsable(s) du traitement concerné(s) à trouver un autre moyen d'apporter des garanties suffisantes concernant les données transférées, par exemple par la signature des clauses contractuelles types 2010/87/UE, et à présenter une nouvelle demande pour ces transferts auprès des autorités compétentes chargées de la protection des données, conformément au droit national applicable.

4.6. Responsabilité

4.6.1. Droit général de recours et, le cas échéant, à une indemnité

Les règles doivent mentionner que les droits de tiers bénéficiaire accordés aux personnes concernées et le droit de recours accordé au responsable du traitement doivent couvrir le recours juridictionnel et le droit à réparation du préjudice subi (pour les personnes concernées, cela doit couvrir le dommage matériel, mais aussi tout préjudice moral).

Pour compléter ce droit général, les règles doivent également contenir des dispositions concernant la responsabilité et la compétence juridictionnelle en vue de faciliter son exercice pratique.

4.6.2. Règles relatives à la responsabilité

4.6.2.1. Règles relatives à la responsabilité pour les personnes concernées

En leur qualité de tiers bénéficiaires, les personnes concernées ont le droit d'opposer les BCR aux filiales du groupe du sous-traitant qui ont enfreint les BCR.

En outre, les BCR applicables aux sous-traitants doivent préciser quel membre du groupe parmi i) le siège européen du sous-traitant, ii) sa filiale européenne responsable par délégation de la protection des données et iii) le sous-traitant européen exportateur de données (en d'autres termes, la partie établie dans l'UE qui conclut le contrat avec le responsable du traitement), accepte d'endosser la responsabilité et de s'engager à prendre les mesures nécessaires pour réparer les actes d'autres filiales établies hors de l'UE (en cas de non-respect des BCR ou du contrat de service) ou de remédier aux violations du contrat écrit (mentionné au point 2.2.2.) commises par un sous-traitant ultérieur externe établi hors de l'UE, ainsi que de verser, s'il y a lieu, une indemnité pour tout préjudice subi. Si l'organisation choisit la troisième option (le sous-traitant européen exportateur de données), elle expliquera à la principale autorité chargée de la protection des données la raison pour laquelle elle ne peut avoir d'entité responsable pour l'ensemble du groupe.

L'entité désignée endosse la responsabilité comme si elle avait commis elle-même l'infraction dans l'État membre dans lequel elle est établie, en lieu et place de la filiale ou du sous-traitant ultérieur externe sis(e) hors de l'UE.

Ladite entité ne peut invoquer un manquement par un sous-traitant ultérieur (que ce dernier fasse ou non partie du groupe) à ses obligations pour échapper à ses propres responsabilités.

Si l'organisation ne dispose d'aucune filiale établie dans l'UE, la responsabilité est endossée par le siège du groupe (sis hors de l'UE).

4.6.2.2. Règles relatives à la responsabilité pour le responsable du traitement

Les BCR applicables aux sous-traitants doivent indiquer que tous les responsables du traitement des données ont le droit d'opposer ces BCR à toute filiale du groupe du sous-traitant en cas d'infraction. Le responsable du traitement devrait également avoir le droit d'opposer le contrat écrit (mentionné au point 2.2.2.) à tout sous-traitant ultérieur externe qui est à l'origine de l'infraction.

En outre, en cas d'infraction commise par une entité du sous-traitant établie hors de l'UE ou par un sous-traitant ultérieur externe établi hors de l'UE, le responsable du traitement doit avoir le droit d'opposer les BCR applicables aux sous-traitants à l'entité du sous-traitant qui a accepté d'endosser la responsabilité[18] de verser une indemnité et de remédier au non-repect des BCR, du contrat de service ou des accords écrits signés avec les sous-traitants ultérieurs externes.

L'organisation doit confirmer, dans son formulaire de demande relatif aux BCR applicables aux sous-traitants, que l'entité qui a accepté d'endosser la responsabilité des actes commis par d'autres filiales liées par les BCR applicables aux sous-traitants à l'extérieur de l'UE ou par un sous-traitant ultérieur externe établi hors de l'UE dispose de ressources financières suffisantes pour verser une indemnité pour le préjudice résultant de la violation des BCR.

4.6.2.3. Règles relatives à la charge de la preuve

Les BCR applicables aux sous-traitants doivent préciser que, lorsque la personne concernée ou le responsable du traitement des données peut démontrer avoir subi un préjudice et établir les faits prouvant que ce préjudice est très probablement le résultat d'une violation des BCR applicables aux sous-traitants (ou du contrat de service ou des contrats écrits mentionnés au point 2.2.2), il appartient à la filiale ayant accepté d'assumer la responsabilité en la matière de prouver que la filiale non européenne du groupe ou le sous-traitant ultérieur externe n'est pas responsable de la violation des BCR qui est à l'origine du préjudice ou qu'aucune violation n'a été commise.

L'entité ayant accepté d'assumer la responsabilité peut s'exonérer de toute responsabilité si elle est en mesure de prouver que la filiale non européenne du groupe n'est pas responsable de l'acte en cause.

4.7. Règle relative à la compétence

Comme il est expliqué au point 4.6.2, l'organisation doit également accepter que les personnes concernées aient le droit d'intenter une action contre l'organisation si elles ne sont pas en mesure d'introduire une plainte contre le responsable du traitement[19], et de choisir l'instance compétente (autorité de protection des données ou tribunal):

a) autorités compétentes chargées de la protection des données, ou

[18] Le siège européen du sous-traitant ou la filiale européenne du sous-traitant responsable par délégation de la protection des données ou le sous-traitant européen exportateur de données (voir section 1.5 du WP195).

[19] Cela peut être le cas lorsque le responsable du traitement a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, à moins que l'ensemble des obligations juridiques du responsable du traitement n'ait été transféré, par contrat ou par l'effet de la loi, au successeur légal, contre lequel la personne concernée peut alors faire valoir ses droits.

b) for de l'entité européenne du sous-traitant qui est à l'origine du transfert, ou

c) for du siège européen du sous-traitant, ou

d) for de la filiale européenne du sous-traitant qui est responsable, par délégation, de la protection des données, ou

e) si l'organisation ne dispose d'aucune filiale établie dans l'UE, les personnes concernées et le responsable du traitement ont le droit d'introduire une plainte auprès des autorités chargées de la protection des données ou des tribunaux de leur lieu de résidence/d'établissement. Si la personne concernée ou le responsable du traitement réside/est établi hors de l'UE et intente une action devant un tribunal non européen, les autorités européennes compétentes chargées de la protection des données doivent être informées de l'existence de cette procédure de contentieux et de son résultat.

Si le système fonctionne bien - ce qui suppose un bon niveau de respect dans l'ensemble du groupe, des audits réguliers, un traitement efficace des plaintes, une coopération avec les autorités de protection des données, etc., l'intervention des tribunaux est peu probable, mais elle ne peut cependant être exclue. Ceci dit, seule l'expérience acquise avec ces instruments nous permettra de savoir si cette prévision est correcte.

Les règles et principes en matière de compétence énoncés dans la directive et dans les législations nationales s'appliquent dûment.

4.8. Transparence

Les organisations liées par les BCR applicables aux sous-traitants doivent être en mesure de prouver que les personnes concernées ont facilement accès à tous les engagements pris au titre des BCR qu'elles ont le droit d'opposer en qualité de tiers bénéficiaires. À cet égard, les BCR applicables aux sous-traitants doivent être publiées sur le site web de l'organisation, d'une manière facilement accessible à toutes les personnes concernées, ou tout au moins un document mentionnant toutes les informations (et non pas un résumé) concernant les droits de tiers bénéficiaire énumérées au point 2.3.3.1.

En ce qui concerne le responsable du traitement, le contrat de service stipulera que les BCR applicables aux sous-traitants font partie intégrante du contrat. Ces BCR seront annexées au contrat de service ou mentionnées dans celui-ci, avec une possibilité d'accès par voie électronique.

5. CONCLUSION

Le groupe de travail estime que les orientations fournies dans le présent document peuvent faciliter l'application de l'article 26, paragraphe 2, de la directive dans le cas des BCR applicables aux sous-traitants. Elles devraient également conduire à une certaine simplification dans les organisations multinationales qui traitent et échangent régulièrement des données à caractère personnel à l'échelle mondiale pour le compte des responsables du traitement.

Le contenu du présent document de travail ne doit pas être considéré comme le dernier mot du groupe de travail «article 29» sur la question mais comme une première étape décisive pour souligner la possibilité d'utiliser les BCR applicables aux sous-traitants dans un cadre

d’autorégulation et de coopération entre les autorités, sans pour autant supprimer la possibilité de recourir à d’autres instruments pour le transfert des données à caractère personnel vers les pays tiers, comme les clauses contractuelles types ou les principes de la «sphère de sécurité», le cas échéant.

D’autres contributions des milieux intéressés et des experts reposant sur l’expérience acquise au sujet de l’utilisation du présent document de travail sont les bienvenues. Le groupe de travail pourrait décider de revenir sur cette question à la lumière de cette expérience.

Fait à Bruxelles, le 19 avril 2013

Pour le groupe de travail

Le président

Jacob Kohnstamm