



**00930/12/FR
WP 195**

**Document de travail 02/2012 établissant un tableau présentant les éléments
et principes des règles d'entreprise contraignantes pour les sous-traitants**

Adopté le 6 juin 2012

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/index_fr.htm

INTRODUCTION

Afin de faciliter l'application des règles d'entreprise contraignantes (ci-après les «BCR») pour les responsables du traitement («BCR pour vos données personnelles»), le groupe de travail «Article 29» a déjà mis au point quelques outils¹ visant à régir les transferts de données à caractère personnel qui sont traitées, à l'origine, par l'entreprise agissant en tant que responsable du traitement (telles que les données relatives aux clients de l'entreprise, à ses salariés, etc.).

Dans le présent document, le groupe de travail «Article 29» entend proposer une boîte à outils décrivant les conditions à respecter, de manière à rendre l'utilisation des BCR plus aisée pour les sous-traitants («BCR concernant les données relatives à des tiers»).

Les BCR pour les sous-traitants visent à définir un cadre pour les transferts internationaux de données à caractère personnel qui sont initialement traitées par l'entreprise en tant que sous-traitant de données, conformément aux instructions externes d'un responsable du traitement des données (notamment pour les activités de sous-traitance).

Conformément à la directive 95/46/CE, un contrat doit être conclu entre le responsable du traitement et le sous-traitant. Ce contrat sera désigné ci-après par l'expression «contrat de service».

¹ Voir WP 153 (boîte à outils pour vérifier toutes les conditions à respecter), WP 155 (questions fréquemment posées) et WP 154 (exemple de BCR), ainsi que les documents de travail WP 74 et 108 (documents de base).

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
1 – CARACTÈRE CONTRAIGNANT			
EN INTERNE			
1.1 L'obligation de respecter les BCR	OUI	OUI	<p>Les BCR doivent clairement indiquer que toutes les filiales du groupe ainsi que ses employés sont tenus de respecter les BCR.</p> <p>En outre, elles doivent préciser expressément que lesdites filiales et les employés du groupe ont aussi 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).</p>
1.2 Une explication sur la manière dont les règles sont rendues contraignantes pour les filiales du groupe et les employés	NON	OUI	<p>Dans son formulaire de demande, le groupe doit expliquer de quelle manière il confère aux règles un caractère contraignant:</p> <p>i) entre les sociétés/entités au sein du groupe, par l'un ou plusieurs des moyens suivants: accord intragroupe, engagements unilatéraux, mesures réglementaires internes, politiques du groupe ou autres moyens;</p> <p>ii) pour les employés, par l'un ou plusieurs des moyens suivants: accord/engagement individuel et distinct, prévoyant des sanctions, clause du contrat de travail prévoyant des sanctions, politiques internes prévoyant des sanctions, ou conventions collectives prévoyant des sanctions.</p>
EN EXTERNE			
1.3 Création de droits de tiers bénéficiaires pour les personnes concernées, avec la possibilité d'introduire une plainte auprès des autorités compétentes chargées de la protection des données et auprès d'un tribunal (choix de la juridiction: for de l'exportateur européen de données du sous-traitant/du siège européen du sous-traitant/de la filiale européenne responsable par délégation de	OUI	OUI	<p>Les BCR doivent garantir aux personnes concernées des droits en matière d'application des règles en qualité de tiers bénéficiaires, pour le cas où la personne concernée ne peut pas porter plainte contre le responsable du traitement des données parce que ce dernier 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 effet de la loi, au successeur légal, contre lequel la personne concernée peut alors faire valoir ses droits.</p> <p>Parmi les droits des personnes concernées, figurent le droit de recours juridictionnel en cas de violation des droits garantis ainsi que le droit à réparation du préjudice subi (dommage matériel, mais aussi tout préjudice moral).</p> <p>Les personnes concernées sont habilitées à déposer plainte devant les autorités chargées de la protection des données ou les tribunaux compétents pour le responsable européen du traitement des données. Si cela se révèle impossible pour les raisons exposées ci-dessus, la personne concernée peut intenter une action devant les</p>

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
la protection des données/responsable européen du traitement des données et, si aucune des situations précitées ne s'applique, juridiction du lieu de résidence de la personne concernée			<p>autorités chargées de la protection des données ou devant le tribunal ayant compétence sur le territoire de l'entité européenne du sous-traitant qui est à l'origine du transfert, du siège européen du sous-traitant ou de la filiale européenne du sous-traitant qui est responsable, par délégation, de la protection des données. Si aucune de ces situations ne s'applique, les personnes concernées ont le droit de déposer plainte auprès du tribunal de leur lieu de résidence. Si la législation nationale prévoit des solutions plus favorables pour la personne concernée, celles-ci peuvent s'appliquer.</p> <p>Les droits de tiers bénéficiaires couvrent les points 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2 et 6.3.</p>
1.4. Responsabilité envers le responsable du traitement	OUI	OUI	<p>Les BCR doivent être rendues contraignantes pour le responsable du traitement grâce à l'introduction d'une référence spécifique à ces règles dans le contrat de service.</p> <p>De plus, les BCR doivent indiquer que tous les responsables du traitement des données ont le droit d'opposer les BCR à toute entité en cas d'infraction. En outre, l'entité visée au point 1.5 assumera la responsabilité du préjudice découlant du non-respect des BCR ou du contrat de service par des filiales non européennes liées par les BCR pour les sous-traitants, ou de la violation du contrat écrit mentionné au point 6.1. vii) par un sous-traitant ultérieur externe établi hors de l'UE.</p> <p>Les droits des responsables du traitement des données incluent le recours juridictionnel et le droit à réparation.</p>
1.5 La société accepte d'endosser la responsabilité d'une éventuelle indemnisation et de remédier aux infractions aux BCR.	OUI	OUI	<p>Les BCR doivent préciser l'obligation, pour le siège européen du sous-traitant, la filiale européenne du sous-traitant responsable par délégation de la protection des données ou l'exportateur européen de données du sous-traitant (en d'autres termes, la partie établie dans l'UE qui conclut le contrat avec le responsable du traitement), 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 et soumises aux BCR, ou de remédier aux infractions commises par un sous-traitant ultérieur externe établi hors de l'UE, ainsi que de verser une indemnité pour tout préjudice résultant de la violation des BCR.</p> <p>L'entité concernée 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.</p> <p>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.</p> <p>Si le sous-traitant soumis aux BCR ne dispose d'aucune filiale établie dans l'UE, la responsabilité est endossée par le siège du groupe (sis hors de l'UE). En pareil cas, 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.</p>

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
1.6 La société dispose de ressources financières suffisantes.	NON	OUI	Le formulaire de demande doit confirmer que l'entité qui a accepté d'endosser la responsabilité des actes commis par d'autres filiales liées par les BCR 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.
1.7 La charge de la preuve incombe à la société et non à la personne concernée.	OUI	OUI	Les BCR 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, 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 ² . 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.
1.8 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	Accès du responsable du traitement aux BCR: le contrat de service dispose que les BCR font partie intégrante du contrat. Les BCR sont annexées au contrat de service ou mentionnées dans celui-ci, avec une possibilité d'accès par voie électronique. Accès de la personne concernée aux BCR: ces dernières sont publiées sur le site internet du groupe du sous-traitant, de manière aisément accessible pour les personnes concernées; si les BCR ne sont pas publiés dans leur intégralité, il convient de diffuser au moins un document incluant toutes les informations (et non un résumé de celles-ci) concernant les points 1.1, 1.3, 1.4, 1.6, 1.7, 2.2, 3.1, 3.2, 4.1, 4.2, 6.1, 6.2 et 6.3.
2 – EFFICACITÉ			
2.1 L'existence d'un programme de formation adéquat	OUI	OUI	Les BCR doivent indiquer qu'une formation adéquate y afférente sera dispensée au personnel ayant un accès permanent ou régulier aux données à caractère personnel et qui participe à la collecte de ces données ou à la mise au point d'outils de traitement de ces données. Au cours de la procédure de demande, les autorités de protection des données qui évaluent les BCR peuvent demander quelques 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	Les BCR doivent indiquer 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 aux BCR sont 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

² Voir aussi FAQ n° 11 du WP 155 applicable aux BCR pour les responsables du traitement.

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
			<p>du traitement).</p> <p>Les BCR doivent préciser que le sous-traitant s'engage à gérer les plaintes déposées par les personnes concernées lorsque le responsable du traitement des données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable.</p> <p>Dans tous les cas où le sous-traitant assure le traitement des plaintes, le département ou la personne chargé(e) de les traiter doit être clairement identifié(e) et jouir d'un niveau adéquat d'indépendance dans l'exercice de ses fonctions.</p> <p>En pareils cas, il convient de fournir aux personnes concernées les informations suivantes:</p> <ul style="list-style-type: none"> - où déposer plainte, - sous quelle forme, - délai de réponse à la plainte, - conséquences en cas de rejet de la plainte, - conséquences si la plainte est jugée recevable, - 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).
<p>2.3 L'existence d'un programme d'audit couvrant les BCR</p>	<p>OUI</p>	<p>OUI</p>	<p>Les BCR doivent imposer au groupe la réalisation, à intervalles réguliers, d'audits en matière de protection des données (par des contrôleurs internes ou externes agréés) ou sur demande expresse du délégué ou de l'instance chargé(e) de la protection des données (ou de toute autre instance compétente au sein de l'organisation).</p> <p>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 place de mesures correctives. En outre, les BCR doivent préciser 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, et sera rendu accessible au responsable du traitement des données.</p> <p>Les BCR doivent mentionner la possibilité, pour les autorités chargées de la protection des données dont relève le responsable du traitement des données, d'avoir accès, sur demande, aux résultats de l'audit; elles doivent, enfin, accorder auxdites autorités l'autorisation ou le pouvoir de mener elles-mêmes des audits sur la protection des données si ceux-ci se révèlent nécessaires et possibles sur le plan juridique.</p> <p>Tout sous-traitant ou sous-traitant ultérieur chargé de gérer les données d'un responsable du traitement particulier accepte de soumettre, à la demande dudit responsable, ses moyens de traitement de données à une</p>

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
			<p>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 secret et choisis par le responsable du traitement, le cas échéant, avec l'accord de l'autorité chargée de la protection des données.</p> <p>Le formulaire de demande inclura une description du système d'audit, précisant par exemple:</p> <ul style="list-style-type: none"> - quelle entité (département au sein du groupe) décide du plan/programme d'audit, - quelle est 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 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 données ou les sous-traitants), les actions correctives, etc.], - quelle est l'entité qui recevra les résultats des audits.
<p>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.</p>	OUI	NON	<p>Engagement à désigner le personnel approprié (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.</p> <p>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 et garantit le respect des règles au niveau global, et selon laquelle les délégués à la protection des données peuvent être chargés 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.</p>
<p>3 – OBLIGATION DE COOPÉRER</p>			
<p>3.1 Une obligation de coopérer avec les autorités de protection des données</p>	OUI	OUI	<p>Les BCR doivent clairement mentionner l'obligation, pour toutes les filiales soumises aux BCR, de coopérer avec les autorités de protection des données dont relève le responsable du traitement concerné, d'accepter de se soumettre à tout audit effectué par celles-ci et de se conformer à leur avis sur toute question ayant trait à ces règles.</p>

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
3.2 Une obligation de coopérer avec le responsable du traitement			Les BCR doivent clairement indiquer l'obligation, pour tout sous-traitant ou sous-traitant ultérieur, de coopérer avec le responsable du traitement et de l'assister afin qu'il se conforme 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 l'obligation d'être en mesure de répondre à une demande 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 - DESCRIPTION DU TRAITEMENT ET DES FLUX DE DONNÉES			
4.1 Une description des transferts couverts par les BCR et de la portée matérielle de celles-ci	OUI	OUI	Les BCR doivent contenir la liste des entités liées par les BCR (voir aussi point 6.2). Le sous-traitant qui soumet des BCR est tenu de fournir à l'autorité de protection des données une description générale de la portée matérielle de ces règles (nature escomptée des données transférées, finalités prévues et importateurs/exportateurs de données dans et hors de l'UE).
4.2 Une déclaration de la portée géographique des BCR (nature des données, type de personnes concernées, pays)	OUI	OUI	Les BCR doivent indiquer qu'il appartient au responsable du traitement d'appliquer les BCR à: i) toutes les données à caractère personnel traitées aux fins des activités du sous-traitant et soumises au droit de l'Union (telles que les données transférées depuis l'Union européenne), OU ii) tous les traitements de données exécutés pour des activités en sous-traitance au sein du groupe, quelle que soit l'origine des données.
5 – MODALITÉS DE COMMUNICATION ET D'ENREGISTREMENT DES MODIFICATIONS			
5.1 Une procédure de mise à jour des BCR	OUI	OUI	Les BCR peuvent être modifiées (<i>par exemple, pour tenir compte des modifications de l'environnement réglementaire ou de la structure de la société</i>) 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 opportun pour permettre à ce dernier de s'y opposer ou de résilier le contrat avant que la modification ne soit effectuée (à titre d'exemple, toutes les modifications prévues concernant le recours à un sous-traitant supplémentaire ou le remplacement d'un sous-traitant doivent être notifiées avant que les

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
			<p>données soient communiquées au nouveau sous-traitant).</p> <p>Les BCR et la liste des filiales soumises aux BCR peuvent être actualisées sans qu'il soit nécessaire d'introduire une nouvelle demande d'autorisation, dans la mesure où les conditions suivantes sont remplies:</p> <ul style="list-style-type: none"> i) une personne désignée tient à jour une 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 disposition du responsable du traitement des données, 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 les informations requises au responsable du traitement de manière systématique 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 et qu'elle n'est pas en mesure de les respecter; iv) toute modification substantielle des BCR 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.

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
-------------------------------------	--------------	-------------------------------	-----------------------------

6 – GARANTIES CONCERNANT LA PROTECTION DES DONNÉES			
<p>6.1 Une description des principes de protection de la vie privée, y compris des règles en matière de transferts ou de transferts ultérieurs en dehors de l'UE.</p>	OUI	OUI	<p>Les BCR doivent inclure les principes suivants, qui seront appliqués par toutes les filiales liées par les BCR:</p> <ul style="list-style-type: none"> i) la transparence et la loyauté: les sous-traitants et sous-traitants ultérieurs sont tenus, de manière générale, d'aider et d'assister le responsable du traitement à respecter la législation (ils ont, par exemple, l'obligation de faire preuve de transparence quant aux activités des sous-traitants ultérieurs, afin de permettre au responsable du traitement d'informer correctement les personnes concernées); ii) la limitation des finalités: l'obligation de traiter les données à caractère personnel pour le compte exclusif du responsable du traitement des données et selon ses instructions. Si la filiale concernée est dans l'incapacité de s'y conformer pour quelque raison que ce soit, elle accepte d'informer dans les meilleurs délais le responsable du traitement des données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert des données et/ou de résilier le contrat. <p>Au terme de la fourniture des services de traitement des données, les sous-traitants et sous-traitants ultérieurs restitueront au responsable du traitement, et à la convenance de celui-ci, l'ensemble des données à caractère personnel transférées ainsi que les copies de ces données, ou détruiront l'ensemble de ces données et en apporteront la preuve au responsable du traitement, à moins que la législation à laquelle ils sont soumis ne les empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. Dans ce cas, les sous-traitants et sous-traitants ultérieurs en informeront le responsable du traitement et garantiront qu'ils assureront la confidentialité des données à caractère personnel transférées et qu'ils ne traiteront plus activement ces données;</p> iii) la qualité des données: les sous-traitants et sous-traitants ultérieurs sont tenus, de manière générale, d'aider et d'assister le responsable du traitement à respecter la législation. Ils ont notamment l'obligation de mettre à exécution: <ul style="list-style-type: none"> - toutes les mesures nécessaires demandées par le responsable du traitement, afin d'assurer la mise à jour, la correction ou la suppression des données. En cas de rectification ou de suppression de données, les sous-traitants et sous-traitants ultérieurs en informent chacune des filiales auxquelles les données ont été divulguées; - toutes les mesures nécessaires demandées par le responsable du traitement, afin de supprimer des données ou de les rendre anonymes dès l'instant où le formulaire d'identification n'est plus requis. En cas de suppression ou d'anonymisation de données, les sous-traitants et sous-traitants ultérieurs en informent chacune des entités auxquelles les données ont été divulguées;

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
			<p>iv) la sécurité: les sous-traitants et sous-traitants ultérieurs doivent se conformer à des mesures de sécurité et d'organisation satisfaisant, à tout le moins, aux exigences imposées par la législation applicable au responsable du traitement, ainsi qu'à toutes les mesures particulières précisées dans le contrat de service. Les sous-traitants et sous-traitants ultérieurs sont tenus d'informer immédiatement le responsable du traitement de tout manquement à la sécurité;</p> <p>v) les droits des personnes concernées: les sous-traitants et sous-traitants ultérieurs mettent à exécution toutes les mesures nécessaires demandées par le responsable du traitement et communiquent à ce dernier toute information utile afin de l'aider à s'acquitter de son obligation de respecter les droits des personnes concernées. En outre, ils transmettront au responsable du traitement toutes les demandes des personnes concernées sans y répondre eux-mêmes, à moins qu'ils n'y soient autorisés;</p> <p>vi) la sous-traitance au sein du groupe: les données peuvent être sous-traitées par d'autres filiales soumises aux BCR, mais uniquement à condition que le responsable du traitement³ en ait été préalablement informé et qu'il y ait donné son consentement écrit préalable. Le contrat de service devra préciser s'il suffit que le responsable du traitement donne son consentement préalable général lors de l'entrée en vigueur du contrat de service ou s'il doit impérativement donner son consentement spécifique à chaque nouvelle opération de sous-traitance. Si un consentement général suffit, le responsable du traitement devra être informé, en temps utile, de tout changement envisagé concernant le recours à un sous-traitant supplémentaire ou le remplacement d'un sous-traitant, de telle sorte qu'il puisse s'opposer audit changement ou résilier le contrat avant que les données soient communiquées au nouveau sous-traitant;</p> <p>vii) les transferts ultérieurs à des sous-traitants ultérieurs externes: les données peuvent être sous-traitées par des entités ne relevant pas du groupe, mais uniquement à condition que le responsable du traitement⁴ en ait été préalablement informé et qu'il y ait donné son consentement écrit préalable. Si un consentement général suffit, le responsable du traitement devra être informé, en temps utile, de tout changement envisagé concernant le recours à un sous-traitant supplémentaire ou le remplacement d'un sous-traitant, de sorte qu'il ait la possibilité de s'y opposer ou de résilier le contrat avant que les données soient communiquées au nouveau sous-traitant.</p>

³ 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.

⁴ 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.

Critères pour l'approbation des BCR	Dans les BCR	Dans le formulaire de demande	BCR pour les sous-traitants
			<p>Si la filiale soumise aux BCR entend sous-traiter les obligations qui lui incombent en vertu du contrat de service, avec le consentement du responsable du traitement, elle ne peut le faire que par voie de contrat conclu par écrit avec le sous-traitant, disposant qu'une protection adéquate est assurée conformément aux articles 16, 17, 25 et 26 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 aux termes du contrat de service et des points 1.3, 1.4, 3 et 6 du présent document de travail.</p>
6.2 La liste des entités liées par les BCR	OUI	OUI	Les BCR doivent inclure la liste des entités liées par ces règles.
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	<p>Les BCR doivent clairement préciser 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 aux termes des BCR ou du contrat de service, elle doit en informer sans délai le responsable du traitement des données (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, de même que l'autorité de protection des données dont relève le responsable du traitement.</p> <p>Toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre doit être communiquée sans délai au responsable du traitement des données, 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 suspendue 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.</p>
6.4 Une déclaration concernant la relation entre la législation nationale et les règles d'entreprise contraignantes	OUI	NON	<p>Il y a lieu de préciser la relation qui existe entre les BCR et la législation applicable en la matière.</p> <p>Les BCR doivent indiquer que, si la législation locale — par exemple, le droit de l'Union — exige un niveau supérieur de protection des données à caractère personnel, celle-ci prime sur les BCR.</p> <p>Dans tous les cas, les données seront traitées conformément au droit applicable.</p>

II. ENGAGEMENTS DEVANT FIGURER DANS L'ACCORD DE NIVEAU DE SERVICE

Les règles d'entreprise contraignantes pour les sous-traitants doivent être liées, sans ambiguïté aucune, à l'accord de niveau de service (ci-après «ANS») signé avec chaque client. Dans cette mesure, il est important de s'assurer que les dispositions de l'ANS incluent les éléments et engagements suivants:

- les BCR sont rendues contraignantes par une référence spécifique à ces règles dans l'ANS (en annexe);
- 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 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.

Fait à Bruxelles, le 6 juin 2012

Pour le groupe de travail
Le président
Jacob KOHNSTAMM