



**18/FR
WP 256 rev.01**

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

**Adopté le 28 novembre 2017
Version révisée et adoptée le 6 février 2018**

Ce groupe de travail a été institué par 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 État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site web: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

INTRODUCTION

Afin de faciliter l'utilisation des règles d'entreprise contraignantes pour les responsables du traitement (Binding Corporate Rules for Controllers, ci-après les «BCR-C») par un groupe d'entreprises ou par un groupe d'entreprises engagées dans une activité économique conjointe pour les transferts internationaux d'organisations établies dans l'UE à des organisations du même groupe établies hors de l'UE, le groupe de travail «Article 29» a modifié le document de travail WP 153 (adopté en 2008) établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes afin de tenir compte des exigences relatives aux règles d'entreprise contraignantes (Binding Corporate Rules, ci-après les «BCR» ou les «règles») désormais énoncées expressément dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, ci-après le «RGPD»)¹.

Il convient de rappeler que les BCR-C ont vocation à encadrer les transferts de données à caractère personnel de responsables du traitement établis dans l'UE à d'autres responsables du traitement ou à des sous-traitants (établis hors de l'UE) au sein du même groupe, tandis que les règles d'entreprise contraignantes pour les sous-traitants (Binding Corporate Rules for Processors ou «BCR-P») s'appliquent aux données reçues d'un responsable du traitement (établi dans l'UE) qui n'est pas une entité du groupe, et ensuite traitées par les entités du groupe concernées en tant que sous-traitants et/ou que sous-traitants ultérieurs. Ainsi, les obligations définies dans les BCR-C s'appliquent aux entités d'un même groupe agissant en qualité de responsables du traitement et aux entités agissant en qualité de sous-traitants «internes». Quant à ces derniers, il y a lieu de rappeler qu'un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui comporte toutes les exigences énoncées à l'article 28, paragraphe 3, du RGPD, doit être signé avec l'ensemble des entreprises sous-traitantes/des sous-traitants internes et externes (par exemple, un contrat de service ou tous autres actes satisfaisant aux mêmes exigences)². En effet, les obligations contenues dans les BCR-C s'appliquent aux entités du groupe recevant des données à caractère personnel en tant que sous-traitants («internes») tant est qu'elles ne soient pas en contradiction avec les dispositions du contrat de service (en d'autres termes, les entités sous-traitantes du groupe traitant ces données au nom des entités du groupe responsables du traitement respecteront en premier lieu les dispositions de ce contrat).

Étant donné que l'article 47, paragraphe 2, du RGPD énonce un ensemble minimum d'éléments à inclure dans les règles d'entreprise contraignantes, le présent tableau modifié vise à:

¹ Texte présentant de l'intérêt pour l'EEE.

² L'article 28, paragraphe 3, du RGPD prévoit notamment que pour chaque relation entre un responsable du traitement et un sous-traitant, soient spécifiés, au moyen d'un contrat ou d'un autre acte juridique, l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. À cet égard, inclure une description générique des catégories de données, des personnes concernées, etc. dans les BCR ne suffira pas.

- adapter la formulation du référentiel précédent de sorte à ce qu'il reste conforme à l'article 47 du RGPD;
- clarifier le contenu nécessaire des BCR spécifié à l'article 47 (en tenant compte des documents WP 74³ et WP 108⁴ adoptés par le groupe de travail «Article 29» dans le cadre de la directive 95/46/CE);
- établir une distinction entre ce qui doit être inclus dans les BCR et ce qui doit être présenté à l'autorité de contrôle compétente dans le cadre d'une demande d'approbation des BCR (document WP 133⁵);
- indiquer les principes auxquels renvoie le texte de l'article 47 du RGPD; et
- fournir des explications/formuler des observations sur chacun de ces principes.

Les documents de travail ayant trait aux BCR, adoptés par le groupe de travail «Article 29», ont manifestement servi de modèle aux auteurs de l'article 47 du RGPD. Toutefois, cet article comporte certains éléments nouveaux dont il conviendra de tenir compte lors de l'actualisation de BCR existantes, ou lors de l'adoption de nouvelles BCR, afin d'en garantir la compatibilité avec le nouveau cadre établi par le RGPD.

1.1 Nouveaux éléments

Dans cette optique, le groupe de travail «Article 29» souhaite plus particulièrement attirer l'attention sur les éléments suivants:

- ***droit d'introduire une réclamation***: les personnes concernées devraient se voir donner le droit d'introduire leur réclamation, selon ce qu'elles décident, soit devant l'autorité de contrôle de l'État membre dans lequel se trouve leur résidence habituelle, leur lieu de travail ou le lieu où la violation aurait été commise (en application de l'article 77 du RGPD), soit devant la juridiction compétente de l'État membre de l'Union (la personne concernée doit pouvoir choisir d'intenter l'action devant les juridictions [de l'État membre] dans lequel l'exportateur de données dispose d'un établissement ou [dans l'État membre] dans lequel la personne concernée réside habituellement) (article 79 du RGPD);
- ***transparence***: toutes les personnes concernées bénéficiant des droits du tiers bénéficiaire devraient en particulier se voir fournir les informations visées aux articles 13 et 14 du RGPD et des informations sur leurs droits à l'égard du traitement et les moyens d'exercer ces droits, sur la clause de responsabilité et sur les clauses portant sur les principes relatifs à la protection des données;
- ***champ d'application***: les BCR précisent la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique

³ Document de travail WP 74: Transferts de données à caractère personnel vers des pays tiers: application de l'article 26, paragraphe 2, de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, adopté le 3 juin 2003, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_fr.pdf.

⁴ 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/article-29/documentation/opinion-recommendation/files/2005/wp108_fr.pdf.

⁵ 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, adopté le 10 janvier 2007, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc.

conjointe et de chacune de leurs entités [article 47, paragraphe 2, point a), du RGPD]. Les BCR doivent également préciser leur champ d'application matériel, par exemple les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers [article 47, paragraphe 2, point b), du RGPD];

- ***principes relatifs à la protection des données***: outre les principes de transparence, de loyauté, de limitation de la finalité, de qualité des données et de sécurité, les BCR devraient également exposer les autres principes visés à l'article 47, paragraphe 2, point d), du RGPD, comme, notamment, les principes de licéité, de minimisation des données, de limitation des durées de conservation des données; les garanties qui accompagnent le traitement de catégories particulières de données à caractère personnel; les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes;
- ***responsabilité***: chaque entité agissant en qualité de responsable du traitement est responsable du respect des BCR et est en mesure de démontrer que celles-ci sont respectées (article 5, paragraphe 2, du RGPD);
- ***législation du pays tiers***: les BCR devraient contenir un engagement selon lequel, dès lors qu'une entité du groupe d'entreprises ou groupe d'entreprises engagées dans une activité économique conjointe est soumise, dans un pays tiers, à une obligation légale susceptible d'avoir un effet négatif important sur les garanties fournies par les BCR, le problème sera communiqué à l'autorité de contrôle compétente (sauf disposition contraire, telle qu'une interdiction à caractère pénal visant à préserver le secret d'une enquête policière). Cela comprend toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité répressive ou d'un organisme de sécurité de l'État.

1.2 Modifications à apporter à des BCR déjà adoptées

Bien que, conformément à l'article 46, paragraphe 5, du RGPD, les autorisations accordées par un État membre ou par une autorité de contrôle sur le fondement de l'article 26, paragraphe 2, de la directive 95/46/CE demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par ladite autorité de contrôle, les groupes disposant de BCR approuvées doivent, en se préparant au RGPD, veiller à la conformité de leurs BCR avec les exigences du RGPD.

Le présent document vise également à aider les groupes disposant de BCR approuvées à mettre en œuvre les modifications pertinentes pour en assurer la conformité avec le RGPD. À cette intention, ces groupes sont invités à notifier les modifications pertinentes apportées à leurs BCR dans le cadre de leur obligation (au titre du point 5.1 du WP 153) à toutes les entités du groupe et aux autorités de protection des données par l'intermédiaire de l'autorité chef de file au titre de leur actualisation annuelle à compter du 25 mai 2018. Ces BCR actualisées peuvent être utilisées sans avoir à faire l'objet d'une nouvelle autorisation ou approbation.

Compte tenu de ce qui précède, les autorités de protection des données se réservent le droit d'exercer leurs pouvoirs au titre de l'article 46, paragraphe 5, du RGPD.

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



Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
1 – CARACTÈRE CONTRAIGNANT EN INTERNE					
1.1 L'obligation de respecter les BCR	OUI	OUI	Article 47, paragraphe 1, point a), et article 47, paragraphe 2, point c), du RGPD	Les BCR doivent être juridiquement contraignantes et imposer une obligation claire à chaque entité participante du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe (ci-après «entité BCR»), y compris à leurs employés, de respecter les BCR.	
1.2 Une explication de la manière dont les règles sont rendues contraignantes pour les entités BCR du groupe ainsi que pour les employés	NON	OUI	Article 47, paragraphe 1, point a), et article 47, paragraphe 2, point c), du RGPD	Dans son formulaire de demande, le groupe doit expliquer de quelle manière il confère aux règles un caractère contraignant: i) à l'égard de chaque entreprise/entité participante du groupe par l'un ou plusieurs des moyens suivants:	

⁶ À remplir par le demandeur.

Ce groupe de travail a été institué par 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 État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site web: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Critères d’approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d’approbation/aux BCR ⁶
				<ul style="list-style-type: none"> - accord intragroupe, - engagements unilatéraux (ceux-ci sont possibles uniquement si l’entité BCR qui prend la responsabilité est située dans un État membre qui admet le caractère contraignant des engagements unilatéraux, et que cette entité BCR a la capacité juridique de lier les autres entités soumises aux BCR), - autres moyens (uniquement si le groupe démontre comment il parvient à garantir le caractère contraignant des BCR); <p>ii) à l’égard des employés, par l’un ou plusieurs des moyens suivants:</p> <ul style="list-style-type: none"> - un ou plusieurs accords/engagements individuels et distincts, prévoyant des sanctions, - clause du contrat de travail spécifiant les sanctions applicables, - politiques internes prévoyant des sanctions, ou - conventions collectives prévoyant des sanctions, - autres moyens (uniquement si le groupe démontre comment il parvient à garantir le caractère contraignant des BCR). 	
EN EXTERNE					
1.3 La création de droits du tiers bénéficiaire pour les personnes concernées. Y compris la	OUI	OUI	Article 47, paragraphe 1, point b),	Les BCR doivent expressément conférer des droits aux personnes concernées leur permettant de se prévaloir des règles en tant que tiers bénéficiaires.	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
<p>possibilité d'introduire une réclamation devant l'autorité de contrôle compétente et devant les juridictions</p>			<p>article 47, paragraphe 2, point c), et article 47, paragraphe 2, point e), du RGPD</p>	<p>Les personnes concernées doivent à tout le moins pouvoir se prévaloir des éléments suivants des BCR:</p> <ul style="list-style-type: none"> - principes relatifs à la protection des données [article 47, paragraphe 2, point d), du RGPD, et section 6.1 du présent référentiel], - transparence et accès aisé aux BCR [article 47, paragraphe 2, point g), du RGPD, et section 6.1 et section 1.7 du présent référentiel], - droits d'accès, de rectification, d'effacement, de limitation, d'objection au traitement, droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage [article 47, paragraphe 2, point e), et articles 15, 16, 17, 18, 21 et 22 du RGPD], - législation nationale empêchant le respect des BCR [article 47, paragraphe 2, point m), du RGPD et section 6.3 du présent référentiel], - droit d'introduire une réclamation selon les procédures internes des entreprises [article 47, paragraphe 2, point i), du RGPD et section 2.2 du présent référentiel], - obligations de coopération avec les autorités de contrôle [article 47, paragraphe 2, points k) et l), du RGPD et section 3.1 du présent référentiel], - dispositions relatives à la responsabilité et à la compétence [article 47, paragraphe 2, points e) et f), du RGPD, et sections 1.3 et 1.4 du présent référentiel]. En particulier, les BCR 	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
				<p>doivent conférer le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente (la personne concernée doit pouvoir choisir l'autorité de contrôle de l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, en application de l'article 77 du RGPD) et devant la juridiction compétente de l'État membre de l'Union (la personne concernée doit pouvoir choisir d'intenter l'action devant les juridictions [de l'État membre] dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement ou [dans l'État membre] dans lequel la personne concernée réside habituellement, en application de l'article 79 du RGPD).</p> <p>Les BCR doivent expressément conférer aux personnes concernées le droit au recours juridictionnel et le droit d'obtenir réparation et, le cas échéant, de recevoir une indemnisation en cas de violation de l'un des éléments exécutoires des BCR énumérés plus haut (voir articles 77 à 82 du RGPD).</p> <p>Les entreprises doivent veiller à ce que l'ensemble de ces droits relèvent de la clause du tiers bénéficiaire de leurs BCR, par exemple en faisant référence aux clauses/sections/parties de leurs BCR qui régissent ces droits, ou en les énonçant tous dans ladite clause du tiers bénéficiaire.</p> <p>Ces droits ne s'étendent pas aux éléments des BCR concernant les mécanismes internes mis en œuvre au sein des entités, tels que le détail des</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
<p>1.4 Le siège européen, l'entité européenne à laquelle les responsabilités en matière de protection des données ont été déléguées ou l'exportateur de données endosse la responsabilité de verser une indemnisation et de remédier aux violations des BCR.</p>	OUI	OUI	Article 47, paragraphe 2, point f), du RGPD	<p>formations, les programmes d'audit, le réseau de conformité, et le mécanisme d'actualisation des règles.</p> <p>Les BCR doivent imposer au siège européen, ou à l'entité européenne responsable par délégation de la protection des données, l'obligation d'endosser la responsabilité des actes d'autres entités du groupe établies en dehors de l'UE et liées par les BCR, de prendre les mesures nécessaires pour réparer ces actes et de verser une indemnité réparatrice du préjudice, matériel ou moral, résultant de la violation des BCR par des entités BCR.</p> <p>Les BCR doivent également indiquer que, dès lors qu'une entité du groupe établie en dehors de l'UE enfreint les BCR, ce cas relève de la compétence des juridictions ou autres autorités compétentes de l'UE, et que les personnes concernées disposent de droits et de recours contre l'entité BCR qui a endossé la responsabilité comme si la violation avait été commise par celle-ci dans l'État membre où elle est établie et non par l'entité du groupe établie en dehors de l'UE.</p> <p>Une autre option, notamment s'il s'avère impossible pour un groupe présentant une structure sociale particulière d'imposer à une entité d'endosser l'entière responsabilité d'une violation des BCR survenue hors de l'UE, est que les BCR prévoient que chaque entité BCR exportant des données hors de l'UE sur le fondement des BCR est responsable des violations des BCR par l'entité BCR établie en dehors de l'UE qui a reçu les données de cette entité BCR européenne.</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
1.5 L'entreprise dispose de ressources financières suffisantes.	NON	OUI	[point 5.5.2. § 2 du WP 74 (page 18) + point 5.17. du WP 108 (page 6)]	Le formulaire de demande doit confirmer que toute entité BCR qui a accepté d'endosser la responsabilité des actes d'autres entités liées par les BCR en dehors de l'UE dispose de ressources financières suffisantes pour verser une indemnité réparatrice des préjudices résultant de la violation des BCR.	
1.6 La charge de la preuve incombe à l'entreprise et pas à l'individu.	OUI	OUI	Article 47, paragraphe 2, point f), du RGPD	Les BCR doivent indiquer que c'est à l'entité BCR qui a accepté d'endosser la responsabilité qu'il incombe de prouver que l'entité BCR établie en dehors de l'UE n'est responsable d'aucune violation des règles ayant entraîné une demande de réparation de la part de la personne concernée. L'entité BCR ayant accepté d'endosser la responsabilité peut être exonérée de toute responsabilité si elle est en mesure de prouver que l'entité BCR établie en dehors de l'UE n'est pas responsable du fait ayant donné lieu au préjudice.	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
1.7 Transparence et accès aisé aux BCR pour les personnes concernées	OUI	NON	Article 47, paragraphe 2, point g), du RGPD	<p>Les BCR doivent prévoir un engagement selon lequel toutes les personnes concernées bénéficiant des droits du tiers bénéficiaire doivent se voir fournir les informations visées aux articles 13 et 14 du RGPD et des informations sur leurs droits à l'égard du traitement et les moyens d'exercer ces droits, sur la clause de responsabilité et sur les clauses portant sur les principes relatifs à la protection des données.</p> <p>Ces informations doivent être fournies dans leur intégralité et un résumé ne suffira pas.</p> <p>Les BCR doivent consacrer le droit des personnes concernées d'y accéder aisément. Par exemple, les BCR peuvent indiquer que, à tout le moins, les parties des BCR à propos desquelles les informations à fournir aux personnes concernées sont obligatoires (voir paragraphe précédent) seront publiées sur l'internet ou sur l'intranet (dès lors que les personnes concernées sont uniquement les membres du personnel de l'entreprise ayant accès à l'intranet).</p>	
2 – EFFICACITÉ					
2.1 L'existence d'un programme de formation adéquat	OUI	OUI	Article 47, paragraphe 2, point n), du RGPD	<p>Les BCR doivent indiquer qu'une formation adéquate y afférente sera dispensée au personnel ayant accès en permanence ou régulièrement aux données à caractère personnel et associé à la collecte de données ou au développement d'outils de traitement des données à caractère personnel.</p> <p>Les autorités de contrôle qui évaluent les BCR peuvent demander à se voir fournir des exemples et des explications sur le programme de formation</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
<p>2.2 L'existence d'un processus de traitement des réclamations concernant les BCR</p>	OUI	OUI	Article 47, paragraphe 2, point i), et article 12, paragraphe 3, du RGPD	<p>au cours de la procédure de demande. Le programme de formation doit être précisé dans la demande.</p> <p>Une procédure interne de traitement des réclamations doit être prévue dans les BCR pour garantir que toute personne concernée peut exercer ses droits et introduire une réclamation concernant une entité BCR.</p> <ul style="list-style-type: none"> - Les réclamations doivent être traitées, dans les meilleurs délais et en tout état de cause dans un délai d'un mois, par un service ou par une personne disposant d'un degré approprié d'indépendance dans l'exercice de ses fonctions, clairement identifié(e). Compte tenu de la complexité et du nombre de demandes, ce délai d'un mois peut être prolongé de deux mois au plus, auquel cas la personne concernée en sera informée. Le formulaire de demande doit expliquer de quelle manière les personnes concernées seront informées des étapes concrètes du système de réclamation, et notamment: <ul style="list-style-type: none"> - où introduire la réclamation, - sous quelle forme, - les délais de réponse à la réclamation, - les conséquences en cas de rejet de la réclamation, - les conséquences si la réclamation est jugée recevable, - les conséquences si la personne concernée n'est pas satisfaite des réponses (droit de former un recours devant une juridiction et d'introduire une réclamation devant l'autorité 	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
2.3 L'existence d'un programme d'audit couvrant les BCR	OUI	OUI	Article 47, paragraphe 2, points j) et l), et article 38, paragraphe 3, du RGPD	<p>de contrôle).</p> <p>Les BCR doivent imposer au groupe l'obligation de faire réaliser des audits en matière de protection des données à intervalles réguliers (par des contrôleurs internes ou externes agréés) ou sur demande expresse du responsable ou de l'instance chargée(e) de la protection de la vie privée (ou de toute autre instance compétente au sein de l'organisation) pour vérifier que cette protection respecte les BCR.</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 œuvre des mesures correctives. En outre, les BCR doivent indiquer que les résultats seront communiqués au responsable ou à l'instance chargée(e) de la protection de la vie privée et au conseil d'administration de l'entreprise qui exerce le contrôle d'un groupe ou du groupe d'entreprises engagées dans une activité économique conjointe. Le cas échéant, les résultats peuvent être communiqués au conseil d'administration de la société mère ultime.</p> <p>Les BCR doivent indiquer que les autorités de contrôle peuvent, sur demande, avoir accès aux résultats de l'audit et doivent donner à celles-ci l'autorité/le pouvoir de réaliser un audit sur la protection des données mise en œuvre par une</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
				<p>entité BCR si nécessaire.</p> <p>Le formulaire de demande inclura une description du système d'audit. Par exemple:</p> <ul style="list-style-type: none"> - quelle entité (quel service 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 spéciale de l'instance chargée de la protection de la vie privée), - le champ couvert par l'audit [par exemple les applications, systèmes informatiques et 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 BCR, l'examen des clauses contractuelles appliquées aux transferts hors du groupe (à des responsables du traitement ou des sous-traitants), les mesures correctives, etc.], - quelle est l'entité qui recevra les résultats des audits. 	
<p>2.4 La création d'un réseau de délégués à la protection des données (DPD) ou de membres du personnel appropriés pour contrôler le respect des règles.</p>	OUI	NON	Article 47, paragraphe 2, point h), et article 38, paragraphe 3, du RGPD	<p>Un engagement de désigner un DPD si nécessaire conformément à l'article 37 du RGPD ou toute autre personne ou entité (telle qu'un responsable en chef de la protection de la vie privée) chargé(e) de contrôler le respect des BCR et ayant le soutien du niveau le plus élevé de la direction pour s'acquitter de cette tâche.</p> <p>Le DPD ou les autres professionnels responsables de la protection de la vie privée peuvent être assistés dans leur tâche d'une équipe, d'un réseau</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
				de DPD locaux ou de contacts locaux le cas échéant. Le DPD fait directement rapport au niveau le plus élevé de la direction (article 38, paragraphe 3, du RGPD). Les BCR doivent inclure une brève description de la structure interne, du rôle, de la fonction et des missions du DPD ou de l'instance similaire, et du réseau créé pour garantir le respect des règles. Par exemple, le fait que le DPD ou le responsable en chef de la protection de la vie privée informe et conseille le niveau le plus élevé de la direction, s'occupe des enquêtes des autorités de contrôle, contrôle et fait rapport annuellement sur le respect des règles au niveau international, et le fait que les DPD locaux ou les contacts locaux peuvent être chargés de traiter les réclamations locales introduites par les personnes concernées, de faire rapport au DPD sur les questions importantes relatives à la protection de la vie privée, de contrôler la formation et le respect des règles au niveau local.	
3 – DEVOIR DE COOPÉRATION					
3.1 Une obligation de coopération avec les autorités de contrôle	OUI	OUI	Article 47, paragraphe 2, point l), du RGPD	Les BCR doivent clairement mentionner l'obligation faite à l'ensemble des entités BCR de coopérer avec les autorités de contrôle, de se soumettre à tout audit réalisé par celles-ci et de se conformer à leur avis sur toute question ayant trait aux règles.	
4 – DESCRIPTION DU TRAITEMENT ET DES FLUX DES DONNÉES					
4.1 Une déclaration du champ d'application matériel des BCR (nature des données transférées, type de personnes concernées,	OUI	OUI	Article 47, paragraphe 2, point b), du RGPD	Les BCR doivent préciser leur champ d'application matériel et, partant, inclure une description générale des transferts de manière à permettre aux autorités de contrôle d'apprécier si	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
pays)				le traitement effectué dans les pays tiers respecte les règles. Les BCR doivent notamment préciser les transferts ou les ensembles de transferts de données, y compris la nature et les catégories de données à caractère personnel, le type de traitement et ses finalités, les types de personnes concernées affectées (données concernant les employés, les clients, les fournisseurs et autres tiers dans le cadre de leurs activités commerciales respectives) et l'identification du ou des pays tiers.	
4.2 Un énoncé du champ d'application géographique des BCR	OUI	OUI	Article 47, paragraphe 2, point a), du RGPD	Les BCR doivent préciser la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe et de chacune de leurs entités. Les BCR doivent indiquer si elles sont applicables: i) à toutes les données à caractère personnel transférées depuis l'Union européenne à l'intérieur du groupe, OU ii) à tous les traitements de données à caractère personnel réalisés au sein du groupe.	
5 – MODALITÉS DE COMMUNICATION ET D'ENREGISTREMENT DES MODIFICATIONS					
5.1 Une procédure d'actualisation des BCR	OUI	OUI	Article 47, paragraphe 2, point k), du RGPD	Les BCR peuvent être modifiées (<i>par exemple, pour prendre en compte les modifications de l'environnement réglementaire ou de la structure de l'entreprise</i>), mais elles doivent imposer l'obligation de communiquer les modifications, dans les meilleurs délais, à toutes les entités BCR et aux autorités de contrôle concernées, par l'intermédiaire de l'autorité de contrôle	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
				<p>compétente.</p> <p>Il est possible d'actualiser les BCR ou la liste des entités BCR sans devoir introduire une nouvelle demande d'approbation, dans la mesure où les conditions suivantes sont remplies:</p> <ul style="list-style-type: none"> i) une personne ou une équipe/un service désigné(e) au sein du groupe actualise la liste des entités BCR, suit et consigne toute actualisation des règles, et fournit les informations requises aux personnes concernées ou aux autorités de contrôle, à leur demande; ii) aucun transfert n'est effectué vers une nouvelle entité BCR tant que celle-ci n'est pas véritablement liée par les BCR et tant qu'elle n'est pas en mesure de les respecter; iii) toute modification des BCR ou de la liste des entités BCR doit être communiquée une fois par an aux autorités de contrôle concernées par l'intermédiaire de l'autorité de contrôle compétente, en même temps qu'une explication succincte des raisons justifiant l'actualisation; iv) dès lors qu'une modification pourrait compromettre le niveau de protection assuré par les BCR ou compromettre de manière significative les BCR (à savoir une modification touchant à leur caractère contraignant), elle sera communiquée sans tarder aux autorités de contrôle concernées par l'intermédiaire de l'autorité de contrôle compétente. 	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
<p>6 – GARANTIES CONCERNANT LA PROTECTION DES DONNÉES</p> <p>6.1.1 Une description des principes relatifs à la protection des données, y compris des règles en matière de transferts ou de transferts ultérieurs hors de l'UE</p>	OUI	OUI	Article 47, paragraphe 2, point d), du RGPD	<p>Les BCR doivent explicitement inclure les principes suivants à respecter par l'entreprise:</p> <ul style="list-style-type: none"> i. transparence, loyauté et licéité [article 5, paragraphe 1, point a), et articles 6, 9, 10, 13 et 14 du RGPD] ii. limitation de la finalité [article 5, paragraphe 1, point b), du RGPD]; iii. minimisation et exactitude des données [article 5, paragraphe 1, points c) et d), du RGPD]; iv. limitation des durées de conservation des données [article 5, paragraphe 1, point e), du RGPD]; v. traitement portant sur des catégories particulières de données à caractère personnel; vi. sécurité [article 5, point f), et article 32 du RGPD], y compris l'obligation de signer avec toute les entreprises sous-traitantes/tous les sous-traitants internes et externes des contrats qui contiennent l'ensemble des exigences énoncées à l'article 28, paragraphe 3, du RGPD, et l'obligation de notifier dans les meilleurs délais toute violation de données à caractère personnel au siège européen ou à l'entité BCR européenne responsable par délégation de la protection des données et aux autres responsable/instance chargé(e) de la protection de la vie privée et personnes concernées dès lors que la violation des données à caractère personnel est susceptible d'engendrer un risque élevé pour leurs droits et libertés. En outre, toute violation de données 	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
				<p>à caractère personnel doit être documentée (en indiquant les circonstances entourant la violation des données à caractère personnel, les effets de cette violation et les mesures correctives prises), et la documentation sera mise à la disposition de l'autorité de contrôle à sa demande (articles 33 et 34 du RGPD);</p> <p>/iii. limitation concernant les transferts et les transferts ultérieurs à des sous-traitants et des responsables du traitement ne faisant pas partie du groupe (les entités BCR responsables du traitement peuvent transférer 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 45, 46, 47 et 48 du RGPD ou qu'une dérogation s'applique au titre de l'article 49 du RGPD).</p>	
6.1.2 Responsabilité et autres outils	OUI	OUI	Article 47, paragraphe 2, point d), et article 30 du RGPD	<p>La formulation et la définition des principes fondamentaux des BCR doivent être conformes à la formulation et aux définitions du RGPD.</p> <p>Chaque entité agissant en qualité de responsable du traitement est responsable du respect des BCR et est en mesure de démontrer que celles-ci sont respectées (article 5, paragraphe 2, et article 24 du RGPD).</p> <p>Afin de démontrer le respect des règles, les entités BCR doivent tenir un registre de toutes les catégories d'activités de traitement, conformément aux exigences énoncées à l'article 30, paragraphe 1, du RGPD. Ce registre doit être tenu par écrit, y compris sous forme électronique, et doit être mis à la disposition de l'autorité de</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
				<p>contrôle à sa demande.</p> <p>Afin de garantir le respect des règles, et si nécessaire, des analyses d'impact relatives à la protection des données doivent être réalisées pour les opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et les libertés des personnes physiques (article 35 du RGPD). Dès lors qu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, l'autorité de contrôle compétente doit être consultée préalablement au traitement (article 36 du RGPD).</p> <p>Il convient de mettre en œuvre des mesures techniques et organisationnelles appropriées, qui sont destinées à concrétiser les principes relatifs à la protection des données et à faciliter le respect des exigences prévues dans les BCR dans la pratique (article 25 du RGPD).</p> <p>Les BCR contiennent une liste des entités qu'elles lient, comprenant leurs coordonnées.</p>	
6.2 La liste des entités liées par les BCR	OUI	OUI	Article 47, paragraphe 2, point a), du RGPD		

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
<p>6.3 Le besoin de transparence dans les cas où la législation nationale empêche le groupe de respecter les BCR</p>	OUI	NON	Article 47, paragraphe 2, point m), du RGPD	<p>Les BCR doivent clairement stipuler que lorsqu'une entité BCR a des raisons de penser que la législation qui lui est applicable risque de l'empêcher de remplir les obligations qui lui incombent en vertu des BCR ou d'avoir un impact négatif sur les garanties fournies, cette entité en informera sans tarder le siège européen ou l'entité BCR européenne responsable par délégation de la protection des données et l'autre responsable/instance chargé(e) de la protection de la vie privée (à moins qu'une autorité répressive ne l'interdise, par exemple en cas d'interdiction à caractère pénal visant à préserver le secret d'une enquête policière).</p> <p>En outre, les BCR doivent contenir un engagement selon lequel, lorsqu'une obligation légale à laquelle est soumise une entité BCR dans un pays tiers est susceptible d'avoir un effet négatif important sur les garanties fournies par les BCR, le problème sera communiqué à l'autorité de contrôle compétente. Cela comprend toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité répressive ou d'un organisme de sécurité de l'État. Dans ce cas, l'autorité de contrôle compétente doit être clairement informée de la demande, y compris des données demandées, de l'organisme demandeur, et du fondement juridique pour la divulgation (sauf disposition contraire, telle qu'une interdiction à caractère pénal visant à préserver le secret d'une enquête policière).</p> <p>Si, dans certains cas particuliers, la suspension et/ou la notification sont interdites, les BCR</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
				<p>prévoient que l'entité BCR à qui la demande a été adressée mettra tout en œuvre pour obtenir le droit d'ignorer cette interdiction afin de communiquer autant d'informations qu'elle peut et dans les plus brefs délais et d'être en mesure de démontrer qu'elle s'est acquittée de cette communication.</p> <p>Si, dans les cas évoqués précédemment, et bien qu'elle ait tout mis en œuvre, l'entité BCR n'est pas en mesure d'informer les autorités de contrôle compétentes, elle doit s'engager dans les BCR à fournir chaque année aux autorités de contrôle des informations générales sur les demandes qu'elle a reçues (par exemple, le nombre de demandes de divulgation, le type de données demandées, le demandeur si possible, etc.).</p> <p>En tout état de cause, les BCR doivent indiquer que les transferts de données à caractère personnel par une entité BCR du groupe à une autorité publique, quelle qu'elle soit, ne peuvent être massifs, disproportionnés et indifférenciés, d'une manière qui excéderait ce qui est nécessaire dans une société démocratique.</p>	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Textes de référence	Remarques	Renvois à la demande d'approbation/aux BCR ⁶
<p>6.4 Une déclaration concernant la relation entre la législation nationale et les BCR</p>	OUI	NON	Sans objet	<p>Les BCR précisent la relation qui existe entre elles et la législation pertinente applicable.</p> <p>Les BCR indiquent que, si la législation locale – par exemple, la législation de l'UE – exige un niveau supérieur de protection des données à caractère personnel, celle-ci prime sur les BCR.</p> <p>En tout état de cause, les données seront traitées conformément au droit applicable, comme le prévoit l'article 5 du RGPD, ainsi qu'à la législation locale pertinente.</p>	