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

18/FR
WP 257 rev.01

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

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

INTRODUCTION

Afin de faciliter l'utilisation des règles d'entreprise contraignantes pour les sous-traitants (Binding Corporate Rules for Processors, ci-après les «BCR "sous-traitants"») 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 d'un même groupe établies hors de l'UE, le groupe de travail «Article 29» (ci-après le «G29») a modifié le document de travail WP 195 (adopté en 2012) 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 expressément énoncées 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»).

Il convient de rappeler que les BCR «sous-traitants» s'appliquent aux données reçues d'un responsable du traitement établi dans l'Union mais n'étant pas membre du groupe, et qui sont ensuite traitées par les membres du groupe agissant en qualité de sous-traitants et/ou de sous-traitants ultérieurs; tandis que les BCR «responsables du traitement» permettent d'encadrer les transferts de données à caractère personnel effectués par des responsables du traitement établis dans l'Union vers d'autres responsables du traitement ou des sous-traitants établis en dehors de l'Union au sein d'un même groupe. Par conséquent, les obligations définies dans les BCR «sous-traitants» s'appliquent lors du traitement de données à caractère personnel de tiers par un membre du groupe agissant en qualité de sous-traitant conformément aux instructions d'un responsable du traitement n'appartenant pas au groupe.

En vertu de l'article 28, paragraphe 3, du RGPD, 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 doit être exécuté entre le responsable du traitement et le sous-traitant. Un tel contrat ou autre acte juridique sera ci-après dénommé «contrat de service».

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:

- adapter la formulation du précédent référentiel de sorte qu'il soit conforme à l'article 47 du RGPD;
- clarifier le contenu nécessaire d'une BCR, conformément à l'article 47 et au document WP 204[1] adopté par le G29 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 195a[2]); et

[1] Document de travail WP204: Document explicatif sur les règles d'entreprise contraignantes pour les sous-traitants, version révisée et adoptée le 22 mai 2015.
[2] Document de travail WP 195a: Recommandation 1/2012 relative au formulaire de demande standard d'approbation des règles d'entreprise contraignantes applicables au transfert des données à caractère personnel à des fins de traitement, adopté le 17 septembre 2012.

- fournir des explications et observations sur chacune des exigences.

Les documents de travail ayant trait aux BCR, adoptés par le G29, ont clairement inspiré la rédaction de l'article 47 du RGPD. Toutefois, cet article comporte certains éléments nouveaux dont il conviendra de tenir compte lors de l'actualisation des BCR existantes déjà approuvées , ou lors de l'adoption de nouvelles BCR, afin d'en garantir la compatibilité avec le nouveau cadre établi par le RGPD.

1. Nouveaux éléments

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

- ***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 conjointe et de chacune de leurs entités [article 47, paragraphe 2, point a), du RGPD]. Les BCR doivent également indiquer 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];

- ***droits des tiers bénéficiaires***: les personnes concernées devraient pouvoir se prévaloir directement des BCR en tant que tiers bénéficiaires auprès du sous-traitant lorsque les exigences en cause incombent spécifiquement aux sous-traitants, conformément au RGPD (articles 28, 29 et 79 du RGPD);

- ***droit d'introduire une réclamation***: les personnes concernées devraient se voir donner le droit d'introduire leur réclamation, à leur convenance, 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 (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);

- ***principes relatifs à la protection des données***: au même titre que les obligations découlant des principes de transparence, de loyauté, de licéité, de limitation de la finalité, de qualité des données et de sécurité, les BCR devraient exposer la façon dont d'autres exigences devront être satisfaites par le sous-traitant, et notamment, en lien avec les personnes concernées, la sous-traitance ultérieure et les transferts ultérieurs vers des entités non liées par les BCR;

- ***obligation de rendre compte***: les sous-traitants seront tenus de mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations leur incombant, notamment au moyen d'audits et d'inspections menées par le responsable du traitement ou par un auditeur mandaté par ce dernier [article 28, paragraphe 3, point h), du RGPD];

- ***contrat de service***: le contrat de service conclu entre le sous-traitant et le responsable du traitement doit contenir tous les éléments requis prévus à l'article 28 du RGPD.

2. Modifications à apporter aux 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 au titre de leur obligation (en vertu du point 5.1 du WP 195) à toutes les entités du groupe et aux autorités de protection des données par l'intermédiaire de l'autorité chef de file dans le cadre de leur actualisation annuelle à partir du 25 mai 2018. Ces BCR actualisées peuvent être utilisées sans avoir à faire l'objet d'une nouvelle autorisation ou approbation des autorités de protection des données.

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.

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
1 – CARACTÈRE CONTRAIGNANT				
EN INTERNE				
1.1 L'obligation de respecter les BCR	OUI	OUI	Les BCR doivent être 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. De plus, les BCR énoncent expressément que chaque entité, y compris ses employés, est tenue de respecter les instructions du responsable du traitement à l'égard du traitement et de la sécurité des données et des mesures de confidentialité contenues dans le contrat de service (articles 28, 29 et 32 du RGPD).	
1.2 Une explication sur la manière dont les règles sont rendues contraignantes pour les entités du groupe et les employés	NON	OUI	Dans son formulaire de demande, le groupe doit expliquer de quelle manière il confère aux règles un caractère contraignant: i) pour chaque entité BCR, par l'un ou plusieurs des moyens suivants: - 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 BCR), - autres moyens (uniquement si le groupe démontre comment il parvient à garantir le caractère contraignant); ii) pour les employés, par l'un ou plusieurs des moyens suivants: - accord/engagement individuel et distinct, prévoyant des sanctions, ou clause du contrat de travail prévoyant des sanctions, - politiques intérieures prévoyant des sanctions, - conventions collectives prévoyant des sanctions,	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			- 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, avec la possibilité d'introduire une plainte aussi bien auprès des autorités de contrôle compétentes qu'auprès d'un tribunal	OUI	OUI	i) Droits directement opposables au sous-traitant Les BCR doivent accorder aux personnes concernées des droits leur permettant de se prévaloir directement des BCR en tant que tiers bénéficiaires auprès du sous-traitant lorsque les exigences en cause incombent spécifiquement aux sous-traitants, conformément au RGPD. À cet égard, les personnes concernées peuvent, à tout le moins, se prévaloir directement des éléments suivants des BCR auprès du sous-traitant: - obligation de respecter les instructions du responsable du traitement concernant le traitement des données à caractère personnel, y compris dans le cadre des transferts de données à caractère personnel vers un pays tiers [article 28, paragraphe 3, points a) et g), et article 29 du RGPD et section 1.1, 6.1.ii et 6.1.iv du présent référentiel], - obligation de mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriées [article 28, paragraphe 3, point c) et article 32 du RGPD et section 6.1.iv du présent référentiel] et de notifier au responsable du traitement toute violation de données à caractère personnel [article 33, paragraphe 2, du RGPD et section 6.1.iv du présent référentiel], - obligation de respecter les conditions lors du recrutement d'un sous-traitant ultérieur faisant partie ou non du groupe [article 28, paragraphe 2, paragraphe 3, point d), et paragraphe 4, et articles 45, 46 et 47 du RGPD et sections 6.1.vi et 6.1.vii du présent référentiel], obligation de coopérer avec le responsable du traitement et de l'aider à respecter et à démontrer qu'il respecte la loi, notamment en ce qui concerne la réponse aux demandes des personnes	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			concernées en lien avec leurs droits [article 28, paragraphe 3, points e), f) et h), et sections 3.2, 6.1.i, 6.1.iii, 6.1.iv, 6.1. v et 6.1. 2 du présent référentiel], - facilité d'accès aux BCR [article 47, paragraphe 2, point g), du RGPD et section 1.8 du présent référentiel], - droit d'introduire une réclamation selon les procédures de réclamation internes [article 47, paragraphe 2, point i), du RGPD et section 2.2 du présent référentiel], - obligation de coopérer avec l'autorité de contrôle [articles 31 et 47, paragraphe 2, point l), du RGPD et section 3.1 du présent référentiel], - dispositions relatives à la responsabilité, à l'obtention d'une indemnisation et à la compétence [articles 47, paragraphe 2, point e), 79 et 82 du RGPD et section 1.3, 1.5 et 1.7 du présent référentiel], - législation nationale empêchant le respect des BCR [article 47, paragraphe 2, point m), du RGPD et section 6.3 du présent référentiel]. ii) Droits opposables au sous-traitant si la personne concernée n'est pas en mesure d'introduire une réclamation contre le responsable du traitement Les BCR doivent expressément conférer aux personnes concernées des droits leur permettant de se prévaloir des BCR en tant que tiers bénéficiaires dans les situations où elles ne sont pas en mesure d'introduire une réclamation contre le responsable du traitement; la raison pouvant être que le responsable du traitement a disparu dans les faits, a cessé d'exister juridiquement ou est devenu insolvable, à moins qu'une entité remplaçante assume l'intégralité des obligations juridiques du responsable du traitement par contrat ou par effet de la loi, auquel cas les	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			personnes concernées peuvent se prévaloir de leurs droits auprès d'une telle entité. Dans un tel cas, les personnes concernées peuvent, à tout le moins, se prévaloir auprès du sous-traitant des sections suivantes du présent référentiel: 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2, 6.3 Les droits des personnes concernées visés aux points i) et ii) couvrent les recours juridictionnels contre toute violation des droits des tiers bénéficiaires garantis ainsi que le droit d'obtenir réparation et, le cas échéant, de recevoir une indemnisation en réparation d'un préjudice (dommage matériel, mais aussi toute souffrance subie). En particulier, les personnes concernées sont autorisées à introduire une réclamation devant l'autorité de contrôle compétente (la personne concernée doit pouvoir choisir l'autorité de contrôle de l'État membre de l'Union dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise) 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). Si le responsable du traitement et le sous-traitant d'un même traitement sont reconnus responsables d'un préjudice causé par ledit traitement, la personne concernée peut percevoir une indemnisation pour l'intégralité des dommages, directement auprès du sous-traitant (article 82, paragraphe 4, du RGPD).	
1.4. Responsabilité envers le responsable du traitement	OUI	OUI	Les BCR sont rendues contraignantes pour le responsable du traitement par une référence spécifique à cet aspect dans le contrat de service, qui satisfait à l'article 28 du RGPD.	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			Par ailleurs, les BCR doivent indiquer que le responsable du traitement a le droit de se prévaloir des BCR auprès de toute entité BCR concernant une violation qu'elle aurait causée et, en outre, auprès de l'entité BCR visée au point 1.5 en cas de violation des BCR ou du contrat de service par des entités BCR établies en dehors de l'Union ou de violation du contrat écrit visé au point 6.1.vii, par tout sous-traitant ultérieur externe établi en dehors de l'Union.	
1.5 La société accepte d'endosser la responsabilité d'une éventuelle indemnisation et de remédier aux infractions aux BCR	OUI	OUI	Les BCR doivent imposer au siège européen du sous-traitant, à l'entité BCR européenne du responsable du traitement à laquelle ont été déléguées les responsabilités en matière de protection des données, ou au sous-traitant exportateur de données (par exemple, la partie européenne ayant conclu un contrat avec le responsable du traitement) l'obligation d'endosser la responsabilité des actes d'autres entités BCR établies en dehors de l'Union et de prendre les mesures nécessaires pour réparer ces actes, de remédier aux violations du sous-traitant ultérieur externe établi en dehors de l'Union, et de verser une indemnisation au titre des dommages résultant d'une violation des BCR. Cette entité BCR acceptera d'endosser la responsabilité comme si la violation avait été causée par elle, dans l'État membre où elle est établie, au lieu de l'entité BCR en dehors de l'UE ou du sous-traitant ultérieur externe établi en dehors de l'Union. Cette entité BCR ne peut invoquer un manquement par un sous-traitant ultérieur (interne ou externe au groupe) à ses obligations pour se soustraire à ses propres responsabilités. S'il n'est pas possible pour certains groupes, dont la structure d'entreprise est particulière, d'imposer à une entité d'assumer la totalité de la responsabilité des violations des BCR en dehors de l'UE, une autre option possible est d'indiquer que chaque entité BCR exportant des données hors de l'Union est responsable des violations des BCR par les sous-traitants ultérieurs (internes ou externes au groupe) établis en dehors de l'Union qui ont reçu les données de cette entité BCR européenne.	
1.6 La société dispose de	NON	OUI	Le formulaire de demande doit confirmer que l'entité qui a accepté	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
ressources financières suffisantes			d'endosser la responsabilité des actes d'autres entités BCR en dehors de l'UE et/ou de tout sous-traitant ultérieur externe établi en dehors de l'Union dispose de ressources financières suffisantes pour verser une indemnité en réparation des préjudices résultant de la violation des BCR.	
1.7 La charge de la preuve incombe à la société et non pas à l'individu	OUI	OUI	Les BCR doivent indiquer qu'il incombe à l'entité qui a accepté d'endosser la responsabilité de prouver que l'entité BCR en dehors de l'Union ou le sous-traitant ultérieur externe ne sont responsables d'aucune violation des règles ayant entraîné une demande de réparation de la part de la personne concernée. Les BCR doivent également indiquer que si le responsable du traitement peut démontrer qu'il a subi des préjudices et présenter des faits montrant que ces préjudices ont probablement été causés par une violation des BCR, il incombe à l'entité BCR du groupe qui a accepté d'endosser la responsabilité de prouver que l'entité BCR en dehors de l'Union ou le sous-traitant ultérieur externe ne sont pas responsables de la violation des BCR entraînant ces préjudices ou que ladite violation n'a pas eu lieu. L'entité ayant accepté la responsabilité peut être exonérée de toute responsabilité si elle est en mesure de prouver que l'entité BCR à l'extérieur de l'UE n'est pas responsable de l'acte.	
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 pour le responsable du traitement: le contrat de service veillera à ce que les BCR fassent partie du contrat. Les BCR seront annexées au contrat de service ou il y sera fait référence, avec la possibilité d'un accès électronique. Accès pour les personnes concernées: les BCR doivent prévoir un engagement selon lequel toutes les personnes concernées bénéficiant des droits du tiers bénéficiaire doivent, en particulier, se voir fournir les informations sur leurs droits de tiers bénéficiaire à l'égard du traitement de leurs données à caractère personnel et sur les moyens d'exercer ces droits. Les BCR doivent stipuler le droit des personnes concernées d'accéder aisément aux BCR. Les parties pertinentes des BCR sont publiées sur le site web du groupe du sous-traitant ou par d'autres moyens adaptés, d'une façon aisément accessible aux personnes concernées ou, au minimum, dans un document comprenant **toutes** (et non un résumé) les	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			informations relatives aux 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, 6.3 du présent référentiel.	
2 –EFFICACITÉ				
2.1 L'existence d'un programme de formation adéquat	OUI	OUI	Les BCR doivent indiquer qu'une formation adéquate sur les BCR sera dispensée au personnel ayant accès en permanence ou régulièrement aux données à caractère personnel et associé à la collecte des données à caractère personnel ou au développement d'outils de traitement de telles données. Au cours de la procédure de demande, les autorités de contrôle qui évaluent les BCR peuvent réclamer des exemples et des explications sur le programme de formation; celui-ci devra être présenté dans la demande.	
2.2 L'existence d'un processus de traitement des plaintes concernant les BCR	OUI	OUI	Les BCR prévoient un engagement selon lequel le groupe du sous-traitant doit créer un point de contact spécifique pour les personnes concernées. Toutes les entités BCR ont le devoir de transmettre toute réclamation ou demande dans les meilleurs délais au responsable du traitement sans être obligées d'y répondre (à moins que le contraire n'ait été convenu avec le responsable du traitement). Les BCR prévoient un engagement selon lequel le sous-traitant doit traiter les réclamations des personnes concernées si le responsable du traitement a disparu dans les faits, a cessé d'exister juridiquement ou est devenu insolvable. Dans tous les cas où le sous-traitant traite des réclamations, celles-ci 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 clairement identifié(e) disposant d'un degré approprié d'indépendance dans l'exercice de ses fonctions. Au regard de la complexité et du nombre de demandes, cette période peut être prolongée de maximum deux mois supplémentaires, et dans un tel cas, la personne concernée doit en être informée. Le formulaire de demande doit indiquer de quelle manière les personnes	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			concernées seront informées des étapes pratiques du système de réclamation, et notamment des éléments suivants: - 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 les personnes concernées ne sont pas satisfaites par les réponses (droit d'introduire un recours auprès d'un tribunal/de l'autorité de contrôle).	
2.3 L'existence d'un programme d'audit couvrant les BCR	OUI	OUI	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 délégué ou de l'instance responsable de la protection des données à caractère personnel (ou de toute autre instance compétente au sein de l'organisation) pour vérifier que cette protection respecte les BCR. 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 délégué ou à l'instance responsable de la protection des données à caractère personnel 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, mais qu'ils seront également rendus accessibles au responsable du traitement. Le cas échéant, les résultats peuvent être communiqués au conseil d'administration de la société mère ultime. Les BCR doivent indiquer que les autorités de contrôle compétentes pour le responsable du traitement 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 entité BCR, si nécessaire. Tout sous-traitant ou sous-traitant ultérieur qui traite des données à caractère personnel pour le compte d'un responsable du traitement en	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			particulier acceptera, à la demande de ce dernier, de soumettre ses moyens de traitement des données à un audit des activités de traitement concernant ce responsable du traitement. Cet audit sera réalisé par le responsable du traitement ou par un organisme d'inspection composé de membres indépendants et en possession des qualifications professionnelles requises, liés par une obligation de confidentialité et sélectionnés par le responsable du traitement, le cas échéant, en accord avec l'autorité de contrôle. Le formulaire de demande inclura une description du système d'audit. Citons quelques exemples: - quelle entité (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 du responsable de la protection des données), - le champ couvert par l'audit [par 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 ou les sous-traitants des données), les actions correctives, etc.], - quelle est l'entité qui recevra les résultats des audits.	
2.4 La création d'un réseau de délégués à la protection des données (DPD) ou de membres du personnel qualifiés pour contrôler le respect des règles	OUI	NON	Un engagement de nommer 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 des données à caractère personnel) chargée de contrôler le respect des BCR. Cette personne/entité bénéficie du niveau de soutien le plus élevé pour l'exercice de cette fonction. Le DPD ou l'autre personne ou entité précitée peuvent, respectivement, être assistés dans l'exercice de cette fonction par une équipe/un réseau 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,	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			paragraphe 3, du RGPD). Une brève description de la structure interne, du rôle, du poste et des tâches du DPD ou fonction similaire, comme indiqué, et de l'équipe/du réseau créé pour garantir le respect des règles. Par exemple, le fait que le DPD ou le responsable en chef de la protection des données à caractère personnel informe et conseille le niveau le plus élevé de la direction, s'occupe des enquêtes des autorités de contrôle, et contrôle et fait rapport annuellement sur le respect des BCR au niveau international, et le fait que les DPD locaux ou les contacts locaux sont chargés de faire rapport au DPD ou au responsable en chef de la protection des données sur les questions principales relatives à la protection des données à caractère personnel, assurant le contrôle de la formation et le respect des règles au niveau local.	
3 – DEVOIR DE COOPÉRATION				
3.1 L'obligation de coopérer avec les autorités de contrôle	OUI	OUI	Les BCR mentionnent clairement l'obligation faite à l'ensemble des entités BCR de coopérer avec les autorités de contrôle compétentes pour le responsable du traitement concerné, de se soumettre à tout audit réalisé par ces autorités et de se conformer à leur avis sur toute question ayant trait aux règles.	
3.2 L'obligation de coopérer avec le responsable du traitement	OUI	OUI	Les BCR mentionnent clairement l'obligation faite à tout sous-traitant ou sous-traitant ultérieur de coopérer avec le responsable du traitement et de l'aider à respecter la législation sur la protection des données (par exemple son obligation de respecter les droits des personnes concernées ou de traiter leurs réclamations, ou d'être en mesure de répondre à une enquête ou à une question des autorités de contrôle). Cette obligation doit être respectée dans un délai raisonnable et dans la mesure où cela est raisonnablement possible.	
4 – DESCRIPTION DU TRAITEMENT ET DES FLUX				

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
DES DONNÉES				
4.1 Une description des transferts et du champ d'application matériel couverts par les BCR	OUI	OUI	Les BCR contiennent une liste des entités BCR, c'est-à-dire des entités qu'elles lient (voir également le point 6.2). Le sous-traitant soumettant une BCR fournit une description générale à l'autorité de contrôle du champ d'application matériel des BCR (nature attendue des données transférées, catégories de données à caractère personnel, types de personnes concernées par les transferts, types attendus de traitement et leurs finalités).	
4.2 Une déclaration de la portée géographique des BCR (nature des données, type de personnes concernées, pays)	OUI	OUI	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 des entités BCR. Les BCR indiquent que le responsable du traitement peut choisir d'appliquer ou non les BCR: i) à toutes les données à caractère personnel traitées dans le cadre des activités du sous-traitant qui sont soumises au droit de l'Union (par exemple, les données transférées depuis l'Union européenne), OU ii) à toutes les données traitées dans le cadre des activités du sous-traitant dans le 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 (par exemple, pour prendre en compte les modifications de l'environnement réglementaire ou de la structure de la société) mais elles doivent prévoir l'obligation de communiquer les modifications à toutes les entités BCR et aux autorités de contrôle pertinentes, par l'intermédiaire de l'autorité de contrôle compétente et du responsable du traitement. Quand une modification influe sur les conditions du traitement, les informations doivent être communiquées au responsable du traitement suffisamment à l'avance pour que ce dernier ait la possibilité de s'opposer à la modification ou de résilier le contrat avant que la modification ne soit	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			apportée (par exemple, pour toute modification prévue concernant l'ajout ou le remplacement de sous-traitants, avant que les données ne soient communiquées au nouveau sous-traitant ultérieur). Les mises à jour des BCR ou de la liste des entités BCR sont possibles sans qu'il soit nécessaire d'introduire une nouvelle demande d'autorisation, dans la mesure où les conditions suivantes sont remplies: i) une personne ou équipe/service défini(e) tient une liste entièrement mise à jour des entités BCR et des sous-traitants ultérieurs participant aux activités de traitement des données pour le responsable du traitement, qui est rendue accessible au responsable du traitement, à la personne concernée et aux autorités de contrôle; ii) cette personne enregistrera et consignera toute mise à jour des règles et fournira systématiquement les informations requises au responsable du traitement ainsi qu'aux autorités de contrôle, à leur demande; iii) 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; iv) toute modification des BCR ou de la liste des entités BCR est communiquée une fois par an aux autorités de contrôle pertinentes par l'intermédiaire de l'autorité de contrôle compétente, assortie d'un bref exposé des motifs la justifiant; v) 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 promptement communiquée aux autorités de contrôle pertinentes par l'intermédiaire de l'autorité de contrôle compétente.	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
6 – GARANTIES CONCERNANT LA PROTECTION DES DONNÉES				
6.1 Une description des principes de confidentialité comprenant les règles sur les transferts ou les transferts ultérieurs en dehors de l'Union	OUI	OUI	Les BCR incluent explicitement les principes suivants à respecter par toute entité BCR: i) Transparence, loyauté et licéité: les sous-traitants et sous-traitants ultérieurs auront l'obligation générale d'aider le responsable du traitement à respecter la loi (par exemple, en l'aidant à être transparent à l'égard des activités du sous-traitant ultérieur pour lui permettre d'informer correctement la personne concernée). ii) Limitation de la finalité: obligation de traiter les données à caractère personnel uniquement pour le compte du responsable du traitement et conformément à ses instructions documentées, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation légale avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public (article 28, paragraphe 3, du RGPD). Dans d'autres cas, si le sous-traitant ne peut respecter ces dispositions pour une raison quelconque, il accepte d'informer promptement le responsable du traitement de son incapacité à s'y conformer, auquel cas le responsable du traitement est autorisé à suspendre le transfert de données et/ou à résilier le contrat. À la résiliation de la prestation des services en lien avec le traitement des données, les sous-traitants et sous-traitants ultérieurs suppriment ou renvoient, selon le choix du responsable du traitement, toutes les données à caractère personnel transférées au responsable du traitement et en suppriment les copies, et certifient à ce dernier avoir exécuté cette tâche, à moins que la législation qui leur est imposée n'exige la conservation des données à caractère personnel transférées. Dans ce cas, les sous-traitants	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			et sous-traitants ultérieurs informeront le responsable du traitement de la situation et lui garantiront d'assurer la confidentialité des données à caractère personnel transférées et de ne plus les traiter activement. iii) Qualité des données: les sous-traitants et sous-traitants ultérieurs auront l'obligation générale d'aider le responsable du traitement à respecter la loi, en particulier: - les sous-traitants et sous-traitants ultérieurs exécuteront les mesures nécessaires lorsque le responsable du traitement en fera la demande, en vue de la mise à jour, de la correction ou de la suppression des données. Les sous-traitants et sous-traitants ultérieurs notifieront les rectifications ou suppressions de données à chaque entité BCR à laquelle les données avaient été communiquées; - les sous-traitants et sous-traitants ultérieurs exécuteront les mesures nécessaires lorsque le responsable du traitement en fera la demande, en vue de la suppression ou de l'anonymisation des données à compter du moment où le formulaire d'identification n'est plus nécessaire. Les sous-traitants et sous-traitants ultérieurs notifieront les suppressions ou anonymisations de données à chaque entité à laquelle les données avaient été communiquées. iv) Sécurité: les sous-traitants et sous-traitants ultérieurs devront mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque que présente le traitement, conformément à l'article 32 du RGPD. Les sous-traitants et sous-traitants ultérieurs devront également aider le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant [article 28, paragraphe 3, point f), du GDPR]. Les sous-traitants et sous-traitants ultérieurs doivent mettre en œuvre des mesures techniques et organisationnelles appropriées qui répondent, au minimum, aux exigences de la législation applicable au responsable du	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			traitement ainsi que toute mesure particulière existante énoncée dans le contrat de service. Les sous-traitants notifient au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. En outre, les sous-traitants ultérieurs sont tenus de notifier au sous-traitant et au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. v) Droits des personnes concernées: les sous-traitants et sous-traitants ultérieurs mettront en œuvre des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, lorsque le responsable du traitement leur en fait la demande, afin d'aider ce dernier à s'acquitter de son obligation de donner suite aux demandes que les personnes concernées lui adressent en vue d'exercer leurs droits prévus au chapitre III du RGPD [article 28, paragraphe 3, point e), du RGPD], y compris en communiquant toute information utile pour aider le responsable du traitement à s'acquitter de son obligation de respecter les droits des personnes concernées. Les sous-traitants et sous-traitants ultérieurs transmettront au responsable du traitement les demandes des personnes concernées sans y répondre, à moins qu'elles ne soient autorisées à le faire. vi) Sous-traitance dans le groupe: les données ne peuvent être sous-traitées par d'autres entités BCR liées par les BCR que si celles-ci disposent de l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement[3]. Le contrat de service précisera si une autorisation préalable générale accordée au début du service suffit ou si	

[3] Informations sur les éléments principaux (parties, pays, sécurité, garanties en cas de transferts internationaux, avec la possibilité d'obtenir une copie des contrats utilisés). Les informations détaillées, comme le nom des sous-traitants ultérieurs, pourraient être fournies dans un registre public numérique, par exemple.

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			une autorisation spécifique sera requise pour chaque nouveau sous-traitant ultérieur. Si une autorisation générale est accordée, le responsable du traitement doit être informé par le sous-traitant de toute modification prévue concernant l'ajout ou le remplacement d'un sous-traitant ultérieur, et ce suffisamment à l'avance pour que le responsable du traitement ait la possibilité de s'opposer à la modification ou de résilier le contrat avant que les données ne soient communiquées au nouveau sous-traitant ultérieur. vii) Transferts ultérieurs vers des sous-traitants ultérieurs externes: les données ne peuvent être sous-traitées par des entités non membres des BCR que si celles-ci disposent de l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement[4]. Si une autorisation générale est accordée, le responsable du traitement doit être informé par le sous-traitant de toute modification prévue concernant l'ajout ou le remplacement de sous-traitants ultérieurs, et ce suffisamment à l'avance pour que le responsable du traitement ait la possibilité de s'opposer à la modification ou de résilier le contrat avant que les données ne soient communiquées aux nouveaux sous-traitants ultérieurs. Lorsque l'entité BCR liée par les BCR sous-traite ses obligations au titre du contrat de service, avec l'autorisation du responsable du traitement, elle a impérativement recours à un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit de l'État membre conclu avec le sous-traitant ultérieur, prévoyant la protection adéquate énoncée aux articles 28, 29, 32, 45, 46 et 47 du RGPD et garantissant que les mêmes obligations de protection des données établies dans le contrat de service entre le responsable du traitement et le sous-traitant et dans les sections 1.3, 1.4, 3 et 6 du présent référentiel sont imposées au sous-traitant ultérieur, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde	

[4] Informations sur les éléments principaux (parties, pays, sécurité, garanties en cas de transferts internationaux, avec la possibilité d'obtenir une copie des contrats utilisés). Les informations détaillées, comme le nom des sous-traitants ultérieurs, pourraient être fournies dans un registre public numérique, par exemple.

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			aux exigences du RGPD (article 28, paragraphe 4, du RGPD).	
6.1.2 Responsabilité *et autres outils*	OUI	OUI	Les sous-traitants seront tenus de mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de leurs obligations prévues à l'article 28, paragraphe 3, point h), du RGPD et pour permettre la réalisation d'audits, y compris des inspections par le responsable du traitement ou un autre auditeur qu'il a mandaté, et y contribuer. De plus, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du RGPD ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données. Afin de démontrer le respect des BCR, les entités BCR doivent tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte de chaque responsable du traitement, conformément aux exigences énoncées à l'article 30, paragraphe 2, 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 contrôle à sa demande (article 30, paragraphes 3 et 4, du RGPD). Les entités BCR aident également le responsable du traitement à mettre en œuvre des mesures techniques et organisationnelles appropriées afin de satisfaire aux principes relatifs à la protection des données et facilitent le respect des obligations fixées par les BCR dans la pratique, comme la protection des données dès la conception et la protection des données par défaut [article 25 et article 47, paragraphe 2, point d), du RGPD].	
6.2 La liste des entités liées par les BCR	OUI	OUI	Les BCR contiennent une liste des entités qu'elles lient, ainsi que leurs coordonnées.	
6.3 Le besoin de transparence dans les cas où la législation nationale empêche le groupe d'observer les BCR	OUI	NON	Un engagement clair selon lequel, 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	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			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, ainsi que l'autorité de contrôle dont relève le responsable du traitement et l'autorité de contrôle dont relève le sous-traitant. Toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité répressive ou d'un organisme étatique de sécurité est communiquée au responsable du traitement, sauf disposition contraire (telle qu'une interdiction pénale visant à préserver le secret d'une enquête policière). Dans tous les cas, la demande de divulgation doit être mise en attente et l'autorité de contrôle dont relève le responsable du traitement ainsi que l'autorité de contrôle dont relève le sous-traitant doivent être expressément informées de la demande, notamment des informations concernant les données demandées, l'organisme demandeur et le fondement juridique pour la divulgation (sauf disposition contraire). Si, dans certains cas particuliers, la suspension et/ou la notification sont interdites, les BCR prévoient que l'entité BCR qui fait l'objet de la demande mette 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. Si, dans les cas évoqués ci-dessus, et bien qu'elle ait tout mis en œuvre, l'entité BCR n'est pas en mesure de notifier les autorités de contrôle compétentes, elle doit s'engager dans les BCR à fournir chaque année aux autorités de contrôle compétentes des informations générales sur les demandes qu'elle reçoit (par exemple, le nombre de demandes de divulgation, le type de données demandées, le demandeur si possible, etc.). 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 sauraient être massifs,	

Critères d'approbation des BCR	Dans les BCR	Dans le formulaire de demande	Remarques	Références à la demande d'approbation/aux BCR
			disproportionnés et sans distinction, ni aller au-delà de ce qui est nécessaire dans une société démocratique.	
6.4 Une déclaration concernant la relation entre la législation nationale et les BCR	OUI	NON	Les BCR précisent la relation entre elles et le droit pertinent applicable. Les règles indiquent que, si la législation locale – par exemple, la législation européenne – exige un niveau supérieur de protection des données à caractère personnel, celle-ci prime les BCR. En tout état de cause, les données sont traitées conformément au droit applicable.	

II. ENGAGEMENTS À PRENDRE DANS L'ACCORD SUR LE NIVEAU DE SERVICE

Les BCR pour les sous-traitants doivent être liées, sans ambiguïté aucune, au contrat de service signé avec chaque client. Dans cette mesure, il est important que les dispositions du contrat de service, qui doivent contenir tous les éléments requis à l'article 28 du RGPD, garantissent ce qui suit:

- les BCR seront rendues exécutoires pour le responsable du traitement (le client) par une référence spécifique à ces règles dans le contrat de service (en annexe);
- le responsable du traitement s'engage, en cas de transfert comprenant des catégories particulières 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 du contrat de service (exempte de toutes informations commerciales sensibles et confidentielles);
- le contrat de service décrit clairement les mesures de confidentialité et de sécurité à respecter ou y renvoie par un lien électronique;
- le contrat de service décrit clairement les instructions et le traitement des données;
- le contrat de service 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.