Règles d'entreprise contraignantes (BCR)

Sous-traitant

SOMMAIRE

ARTICLE 2 : DÉFINITIONS

Lorsqu'ils commencent par une lettre capitale, les termes suivants ont la signification qui leur est attribuée ci-dessous :

« **Pays tiers adéquat** » : un pays qui n'est pas membre de l'Espace économique européen et qui a été reconnu comme garantissant un niveau approprié de des Données à caractère personnel par la Commission européenne conformément à l'Article 45 du RGPD ;

« **Entité(s) BCR** » : une Entité ou des Entités qui s'engage(nt) à respecter les présentes BCR en les signant, soit en qualité d'Exportateur de Données soit en qualité d'Importateur de Données ;

« **Client(s)** » : la personne physique ou morale qui a signé un Contrat de Service avec une entité du Groupe Leyton ;

« Responsable(s) du Traitement » le(s) Client(s) qui détermine(nt) les Finalités et les moyens du Traitement ;

« **Exportateur de Données** » : une Entité ou des Entités du Groupe Leyton située(s) dans l'Espace économique européen qui transfère(nt) des Données à caractère personnel vers un Pays tiers en qualité de Sous-traitant ;

« **Importateur de Données** » : une Entité du Groupe Leyton établie dans un Pays tiers et qui reçoit les Données aux fins de leur traitement en sa qualité de Sous-traitant ou de Sous-traitant ultérieur ;

DPO (de l'anglais « Data Protection Officer ») : la personne déléguée pour la protection des données, établie par les Articles 37 et suivants du RGPD ; pour les entités qui sélectionneront ou ont déjà désigné un DPO, cette personne sera notamment chargée de donner des conseils et des informations ainsi que de contrôler le respect, au sein de l'Entité, des règles résultant du RGPD ;

« Réglementations applicables en matière de protection des Données » : l'ensemble composé du RGPD et de la Loi informatique et libertés ou de toute autre législation nationale spécifique concernant la protection des Données à caractère personnel qui est applicable à chaque Entité, sur laquelle l'Importateur de Données convient que le RGPD prévaudra en cas de contradiction ;

« **Personne concernée** » : une personne physique à laquelle se rapportent les Données faisant l'objet du Traitement ;

« **Entités** » : désigne :

- Thésée, société par actions simplifiée de droit français dont le siège social est sis 16 boulevard Garibaldi, 92230 ISSY LES MOULINEAUX, immatriculée au Registre du Commerce et des Sociétés de Nanterre sous le numéro 504 868 399 (ci-après désignée « Thésée ») ;
- Toute société contrôlée par, ou contrôlant, Thésée, au sens de l'Article L.233-3 du Code de commerce.

« L'espace économique européen » ou « EEE » : les États membres de l'Union européenne (UE) et trois pays de l'Association européenne de libre-échange (AELE) (Islande, Liechtenstein et Norvège ; à l'exclusion de la Suisse).

« **RGPD** » 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 de données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE ;

« **Groupe Leyton** » : désigne toutes les Entités ;

« **État(s) membre(s)** » : État(s) membre(s) souverain(s) de l'Espace économique européen ;

« **Commission nationale de l'informatique et des libertés »** ou la « **CNIL** » : l'Autorité de contrôle française qui est l'Autorité de contrôle chef de file pour les BCR ;

« Données à caractère personnel » ou « Données » : toutes informations concernant une personne physique qui peuvent permettre l'identification de cette personne directement ou indirectement, telles que - par exemple - un nom de famille, un prénom, des initiales, des photos, un numéro de badge ou une adresse IP ;

« **Violation de Données à caractère personnel »** : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

« Personnel » : toute personne physique qui est un employé, un stagiaire ou autre et qui travaille pour le compte de l'une des Entités du Groupe Leyton, à l'exclusion du Sous-traitant ultérieur ;

« **Traitement de Données à caractère personnel** » : toute opération ou tout ensemble d'opérations effectuées à l'initiative du Responsable du Traitement et appliquées à des Données, quelle que soit la procédure utilisée, et en particulier la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le

rapprochement ou l'interconnexion, ainsi que la limitation, l'effacement ou la destruction ;

« Finalité(s) » : l'objectif visé par le Traitement. En d'autres termes, les raisons pour lesquelles les données ont été collectées par le Responsable du Traitement ;

« Service(s) » : toute opération réalisée pour le compte des Clients du Groupe Leyton consistant en :

- la prestation de services de conseil en matière fiscale et d'ingénierie sociale, en particulier au moyen d'une recherche de financement, d'une optimisation des charges sociales, taxes et achats (téléphonie, flotte automobile, personnel temporaire, assurance, énergie, etc.) ;
- l'évaluation de certificats énergétiques et la prestation de services de conseil en matière d'économies d'énergie ;
- la prestation de services externalisés dans le domaine des ressources humaines et de la facturation/du recouvrement de créances auprès de Clients.

« **Contrat de service** » : Le Contrat conclu entre le Client et une Entité du Groupe Leyton et qui porte sur l'exécution des Services, dont les présentes BCR font partie intégrante ;

« Sous-Traitant » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel sur les instructions et pour le compte du Responsable du Traitement ;

« Sous-traitant ultérieur » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui est engagé par le Sous-traitant pour traiter les Données à caractère personnel conformément aux instructions et pour le compte du Responsable du Traitement. Le Sous-traitant ultérieur peut être interne ou externe au Groupe Leyton ;

« **Autorité(s) de contrôle** » : l'autorité ou les autorités publique(s) indépendante(s) instituée(s) au sein de chaque État membre de l'EEE pour protéger les libertés et droits fondamentaux des personnes physiques à l'égard du Traitement de Données à caractère personnel au sein de l'EEE ;

« **Pays tiers** » : un pays qui n'est pas membre de l'EEE et qui n'a pas été reconnu comme garantissant un niveau approprié de protection des Données à caractère personnel par la Commission européenne conformément à l'Article 45 du RGPD ;

« Transfert de Données à caractère personnel » ou « Transfert » : tout(e) accès à, communication, copie ou déplacement des Données à caractère personnel afin qu'elles soient traitées dans un Pays tiers.

ARTICLE 3 : PRÉSENTATION DU GROUPE LEYTON

La structure du Groupe Leyton, ainsi que l'identité et les coordonnées de chaque Entité le composant sont indiquées en Annexe 1 aux présentes BCR.

Cette Annexe pourra être mise à jour en cas d'évolution de la structure du Groupe Leyton et sera communiquée à l'Autorité de contrôle, sans qu'il soit nécessaire de soumettre cette nouvelle version de l'Annexe 1 pour signature à chaque Entité qui est déjà partie aux BCR.

ARTICLE 4 : CHAMP D'APPLICATION

Article 4.1: CHAMP D'APPLICATION MATERIEL

Les présentes BCR sont contraignantes pour toutes les Entités du Groupe Leyton, qu'elles soient Importatrice de Données ou Exportatrice de Données, qui se sont engagées à les respecter et qui ont signé le formulaire d'adhésion figurant en Annexe 0, et dont la liste figure en Annexe 1. En cas de modification, les règles qui seront appliquées sont décrites à l'ARTICLE 11 :

Article 4.2: CHAMP D'APPLICATION TERRITORIAL

Les présentes BCR s'appliquent aux Entités BCR établies dans un pays de l'EEE exportant des Données à caractère personnel directement ou indirectement, et aux Entités BCR non établies dans un pays de l'EEE important les Données à caractère personnel. Les BCR s'appliquent aux premiers Transferts de Données à caractère personnel et aux Transferts ultérieurs.

Les BCR ne s'appliquent ni aux Transferts de données entre Entités situées dans un Pays tiers adéquat ou dans un État membre de l'EEE ni vers Entités situées dans un Pays tiers adéquat ou dans un État membre de l'EEE.

ARTICLE 5 : DESCRIPTION DES ACTIVITÉS DE TRAITEMENT

Article 5.1: DESCRIPTION DU TRAITEMENT

Certains Services fournis aux Clients peuvent être sous-traités à des Entités du Groupe LEYTON qui sont situées dans un Pays tiers, et donc impliquer des Transferts de Données à caractère personnel collectées par des Clients qui sont des Responsables du Traitement.

En fonction de la nature des Services convenus avec le Client, ces Services sous-traités peuvent impliquer les opérations de traitement suivantes :

- Collecte ;
- Extraction ;

- Conservation ;
- Enregistrement ;
- Utilisation ;
- Organisation ;
- Structuration ;
- Adaptation ou modification ;
- Rapprochement ou interconnexion ;
- Limitation ;
- Transfert ;
- Consultation ;
- Communication par transmission ;
- Diffusion ou toute autre forme de mise à disposition ;
- Destruction ;
- Suppression.

Article 5.2: FINALITES

Les Traitements nécessitant le Transfert de Données à caractère personnel à des Entités situées dans un Pays tiers poursuivent pour tout ou partie des Finalités nécessaires à la fourniture des Services souscrits lesquels portent sur la collecte indirecte (en provenance du Sous-traitant initial), puis l'extraction, l'enregistrement, la structuration, l'analyse et l'audit des données, leur contrôle/vérification, leur adaptation (et leur correction, si nécessaire), leur diffusion par la restitution au Sous-traitant et au Responsable du Traitement, leur conservation pendant la durée nécessaire puis leur destruction à l'issue de cette période, dans le cadre de Services portant sur :

(i) accompagnement en matière d'économies ou de leviers de financements générés notamment par :

(i.1) Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« **CIR** ») et les aides et subventions ;
(i.2) la livraison de Certificat d'économie d'énergie (« **CEE** ») ou autre dispositif national de certificats blancs ;
(i.3) l'optimisation de la fiscalité locale et nationale ;
(i.4) l'optimisation de la fiscalité des entreprises ;
(i.5) l'optimisation de la fiscalité sur l'énergie ;
(i.6) l'optimisation des charges sociales et du financement de la formation ;
(i.7) l'optimisation des charges locatives ;
(i.8) l'optimisation de l'affectation des ressources de la société (télécommunications, Flotte automobile, intérim, dépenses énergie, assurances, etc.)

(ii) le recouvrement d'indemnités journalières des salariés des Clients (« **IJSS** et **IJP**»), du versement de la contribution « Versement Transport » (« **VT** ») auxquelles sont soumis des Clients, la gestion des Visites médicales (« **VM** »), des formations et des déclarations d'Accidents du Travail (« **AT** »);

(iii) la fourniture et la maintenance de logiciels ;
(iv) l'analyse et le contrôle du traitement des factures et du recouvrement d'espèces.

Article 5.3: CATEGORIES DE DONNEES A CARACTERE PERSONNEL

Les catégories de Données à caractère personnel qui peuvent être transférées sont les suivantes :

a) Informations d'identification (prénom, nom de famille, date et lieu de naissance ; Numéro de sécurité sociale) ;
b) Données relatives à la vie privée (adresse, coordonnées, nombre d'enfants, situation matrimoniale, etc.) ;
c) Données relatives à la vie professionnelle (intitulé du poste, curriculum vitae, numéro de matricule, informations relatives à la paie, informations relatives à la formation, etc.) ;
d) Données relatives à la vie économique et financière (Numéro d'identification fiscale, etc.) ;
e) Données relatives à la santé (informations relatives à un accident du travail et aux arrêts maladie, etc.).

Article 5.4: CATEGORIES DE PERSONNES CONCERNEES

Les catégories de Personnes concernées par le Transfert de leurs Données à caractère personnel sont les suivantes :
(i) le personnel des Clients (salariés, travailleurs temporaires, stagiaires, etc.) ;
(ii) les partenaires contractuels des Clients ou leurs représentants et leurs Clients potentiels, le cas échéant ;
(iii) les tiers susceptibles d'intervenir dans le cadre des Services (en particulier les auxiliaires de justice, représentants nommés par un tribunal, etc.).

ARTICLE 6 : OBLIGATIONS DES ENTITÉS BCR

Article 6.1: CONFORMITE AUX PRESENTES BCR

6.1.1. CONFORMITE PAR LES ENTITES BCR

Toutes les Entités BCR s'engagent à se conformer rigoureusement aux présentes BCR, ainsi qu'aux stipulations relatives au Traitement de Données à caractère personnel, et aux mesures de sécurité et de confidentialité figurant dans les Contrats de Service conclus avec les Responsables du Traitement.

Toute disposition résultant des Réglementations applicables en matière de protection des Données qui serait plus stricte que les stipulations des présentes BCR prévaudra.

Les Entités BCR s'engagent à informer dans les meilleurs délais le Responsable du Traitement, Thésée, ainsi que l'Autorité de contrôle compétente à l'égard du Responsable du Traitement et l'Autorité de contrôle chef de file compétente à l'égard du Sous-traitant, de toute obligation actuelle ou à venir imposée par les Réglementations applicables en matière de protection des Données qui :
(i) pourrait empêcher une Entité BCR d'exécuter les instructions reçues du Responsable du Traitement ou ses obligations résultant des BCR ou du Contrat de Service ; et/ou
(ii) pourrait avoir une incidence négative sur l'application des présentes BCR.

Le Responsable du Traitement est en droit de suspendre le Transfert de données et/ou de résilier le contrat.

Toute demande contraignante de divulgation des Données à caractère personnel émanant d'une autorité répressive ou d'un organisme de sécurité d'État doit être communiquée au Responsable du Traitement, sauf disposition contraire (telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière). En tout état de cause, la demande de divulgation doit être mise en attente et l'Autorité de contrôle compétente à l'égard du Responsable du Traitement et l'Autorité de contrôle compétente à l'égard du Sous-traitant doivent être clairement informées de la demande, ainsi que des caractéristiques de celle-ci : données concernées, Autorité ayant formulé la demande et base légale de la demande (sauf en cas d'interdiction).

Dans certains cas spécifiques dans lesquels la suspension et/ou la notification sont interdites, l'Entité BCR ayant reçu la demande fera tout son possible pour obtenir une renonciation à cette interdiction afin de communiquer autant d'informations que possible et dès que possible et devra être en mesure de démontrer qu'elle l'a fait.

Si, dans les cas visés ci-dessus, bien qu'elle ait fait tout son possible, l'Entité BCR ayant reçu la demande n'est pas en mesure d'aviser l'Autorité de contrôle

compétente, des informations générales sur les demandes reçues par l'Entité doivent être transmises chaque année à l'Autorité de contrôle compétente (par ex. nombre de demandes de divulgation, type de données demandées, auteur de la demande, si possible, etc.).

En tout état de cause, les Transferts de Données à caractère personnel par une Entité BCR à toute autorité publique ne doivent pas être massifs, disproportionnés et inconsidérés, d'une manière qui irait au-delà de ce qui est nécessaire dans une société démocratique.

Pour les Entités BCR situées dans l'EEE, tout jugement d'une cour ou d'un tribunal et toute décision d'une autorité administrative d'un Pays tiers imposant à un Responsable du Traitement ou à un Sous-traitant de transférer ou divulguer des Données à caractère personnel ne peut être reconnu(e) ou exécutoire de quelque manière que ce soit que s'il/si elle est basé(e) sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le Pays tiers demandeur et l'Union ou un État membre de l'EEE, sans préjudice d'autres motifs de transfert prévus par le Chapitre V du RGPD.

6.1.2. OBLIGATIONS DU PERSONNEL

6.1.2.1. RESPECT DES BCR ET DES CONTRATS DE SERVICE

Toutes les Entités BCR doivent garantir que leur Personnel autorisé à accéder aux Données des Clients ou à les traiter se conforme :
(i) aux présentes BCR, qui leur ont été communiquées au préalable ;
(ii) aux instructions reçues des Responsables du Traitement, en particulier en ce qui concerne la sécurité et la confidentialité des Données et qui sont énoncées dans les Contrats de Service. À ce titre, les Entités BCR s'engagent à communiquer à leurs employés, en temps utile, toutes les instructions nécessaires à l'exécution du Traitement.

6.1.2.2. ENGAGEMENTS AU TITRE DE LA CONFIDENTIALITE ET DE LA SECURITE DES DONNEES PRIS PAR LE PERSONNEL

Toutes les Entités BCR doivent veiller à ce que le Personnel autorisé à accéder aux Données des Clients ou à les traiter soit soumis à une obligation de confidentialité.

Article 6.2: COMMUNICATIONS

Les Entités BCR doivent communiquer les réclamations et demandes des Personnes concernées dans les meilleurs délais (i) directement au Responsable du Traitement ou, (ii) indirectement par l'intermédiaire du DPO ou de l'Exportateur de Données.

Article 6.3: SECURITE ET CONFIDENTIALITE DES DONNEES

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des Finalités du Traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des Personnes concernées, les Entités BCR doivent mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité des Données adapté aux risques, y compris entre autres, selon les besoins :

(i) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

(ii) des moyens permettant de rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

(iii) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du Traitement.

Une description des mesures de sécurité figure en Annexe 3.

Ces mesures devront répondre au moins aux prescriptions du droit applicable au Responsable du Traitement et à toutes mesures existantes particulières spécifiées dans le Contrat de Service signé avec le Responsable du Traitement.

Article 6.4: PROCEDURE DE NOTIFICATION EN CAS DE VIOLATION DE DONNEES A CARACTERE PERSONNEL

Les Entités BCR s'engagent à, directement ou indirectement par l'intermédiaire de l'Exportateur de Données, informer les Responsables du Traitement dès que possible après avoir pris connaissance de toute Violation de Données à caractère personnel. En tout état de cause, les Entités BCR doivent aider les Responsables du Traitement en leur transmettant toutes les informations utiles en leur possession ou liées à une Violation de Données à caractère personnel.

Article 6.5: CONFORMITE AUX INSTRUCTIONS DES RESPONSABLES DU TRAITEMENT

Si un Transfert vers un Pays tiers ou à une organisation internationale est requis en vertu du droit de l'Union européenne ou du droit d'un État membre, l'Exportateur de Données doit, immédiatement et avant que le Traitement ait lieu, en informer le Responsable du Traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Les Entités BCR ne doivent traiter les Données à caractère personnel pour le compte des Responsables du Traitement que selon leurs instructions documentées et s'engagent à s'y conformer rigoureusement. Si une Entité BCR

est dans l'incapacité de s'y conformer pour quelque raison que ce soit, elle doit en informer immédiatement le Responsable du Traitement, soit directement soit indirectement par l'intermédiaire de l'Exportateur de Données. Dans ce cas, le Responsable du Traitement peut suspendre le Transfert des Données jusqu'à ce qu'une solution soit trouvée conjointement ou résilier le contrat.

Article 6.6: AIDE ET ASSISTANCE DES RESPONSABLES DU TRAITEMENT

6.6.1. RESPECT DES REGLEMENTATIONS APPLICABLES EN MATIERE DE PROTECTION DES DONNEES

Les Entités BCR doivent collecter, conserver et mettre à la disposition du Responsable du Traitement toutes les informations nécessaires pour permettre au Responsable du Traitement de démontrer le respect des obligations qui lui incombent en vertu des Réglementations applicables en matière de protection des données. Les Entités BCR doivent aider le Responsable du Traitement à répondre à toute enquête ou demande de renseignements des Autorités de contrôle.

Les Entités BCR et les Sous-traitants ultérieurs externes s'engagent à

i) transmettre, dès que possible, au Responsable du Traitement toutes les informations nécessaires aux fins d'une analyse d'impact de la manière prescrite par les Articles 35 et suivants du RGPD, et qu'il pourrait ne pas avoir en sa possession et qu'il pourrait ne pas être en mesure d'obtenir lui-même.

ii) aider le Responsable du Traitement à garantir le respect des obligations prévues aux Articles 32 à 36 du RGPD, compte tenu de la nature du Traitement et des informations à la disposition du Sous-traitant.

iii) faciliter le respect par le Responsable du Traitement des principes de protection des données dès la conception et par défaut.

Les Entités BCR doivent coopérer avec le Responsable du Traitement et l'aider à s'acquitter de son obligation de respecter les droits des Personnes concernées et de donner suite à leurs réclamations. Les Entités BCR doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires pour aider les Responsables du Traitement, à leur demande, à mettre à jour, corriger ou supprimer les Données. Les Entités BCR et les Sous-traitants ultérieurs prendront toutes mesures nécessaires, à la demande du Responsable du Traitement, pour faire supprimer ou anonymiser les données dès lors qu'elles ne sont plus nécessaires sous une forme permettant l'identification. Les Entités BCR et les Sous-traitants ultérieurs communiqueront à chaque Entité à laquelle les données auront été divulguées toute demande de rectification, de suppression ou d'anonymisation de données.

En outre, si l'Entité BCR estime qu'une Instruction est contraire au RGPD ou à toutes autres prescriptions du droit de l'Union ou d'un État membre de l'EEE en

matière de protection des données, elle devra en informer le Responsable du Traitement immédiatement.

Afin de démontrer le respect des BCR, les Entités BCR doivent conserver un registre de toutes les catégories d'activités de Traitement effectuées pour le compte de chaque Responsable du Traitement, contenant les informations indiquées à l'Art. 30.2 du RGPD. Ce registre doit se présenter sous une forme écrite, y compris la forme électronique, et doit être mis à la disposition de l'Autorité de contrôle sur demande.

6.6.2. DEMANDES DES PERSONNES CONCERNEES

Les Entités BCR doivent transmettre toutes demandes émanant de Personnes concernées par le Traitement dans les meilleurs délais et dans un délai maximum de 5 jours ouvrés, directement aux Responsables du Traitement ou, si nécessaire, indirectement par l'intermédiaire de l'Exportateur de Données.

Elles doivent également mettre en place des mesures techniques et organisationnelles appropriées, dans la mesure du possible, afin de les aider à répondre à ces demandes dans les meilleurs délais, y compris en communiquant toutes informations utiles pour aider le Responsable du Traitement à s'acquitter de son obligation de respecter les droits des Personnes concernées.

Article 6.7: SOUS-TRAITANT ULTERIEUR

Les Entités BCR doivent se conformer aux Réglementations applicables en matière de protection des Données et aux stipulations énoncées dans les Contrats de service régissant le Traitement des Données à caractère personnel qu'elles traitent pour le compte des Responsables du Traitement.

À cette fin, elles doivent :
(i) s'abstenir de sous-traiter les Services impliquant le Traitement de Données à caractère personnel sans avoir obtenu l'autorisation générale ou spécifique du Responsable du Traitement ;
(ii) si nécessaire, communiquer fidèlement et en temps opportun les instructions de traitement du Responsable du Traitement au Sous-traitant ultérieur.

L'Entité BCR doit obtenir l'autorisation écrite préalable générale éclairée du Responsable du Traitement pour désigner un Sous-traitant ultérieur pour le traitement de Données à caractère personnel. L'Entité BCR soumettra au Responsable du Traitement une liste exhaustive des Sous-traitants ultérieurs, sur demande du Responsable du Traitement, et informera le Responsable du Traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres Sous-traitants ultérieurs afin de donner au Responsable du Traitement la possibilité d'émettre des objections à l'encontre de ces changements ou de

résilier le contrat avant que les données ne soient communiquées au nouveau Sous-traitant ultérieur.

Une Entité BCR ne peut désigner un Sous-traitant ultérieur externe pour traiter des Données à caractère personnel que si une évaluation des risques pour la vie privée et la sécurité a été réalisée afin de déterminer que ledit Sous-traitant ultérieur donnera des garanties suffisantes qu'il mettra en œuvre des mesures techniques et organisationnelles appropriées et se conforme aux Réglementations applicables en matière de protection des Données de l'EEE.

L'Entité BCR doit veiller à ce qu'il existe un contrat écrit avec le Sous-traitant ultérieur, reconnu comme valable en vertu des Réglementations applicables en matière de protection des Données de l'EEE et contenant :

- les dispositions énoncées dans les Articles 28, 29 et 32 du RGPD ;
- les dispositions énoncées dans les Articles 45, 46 ou 47 du RGPD ;
- la création de droits de tiers bénéficiaires pour les Personnes concernées ; y compris la possibilité d'introduire une réclamation devant l'Autorité de contrôle compétente et devant les tribunaux
- une responsabilité envers le Responsable du Traitement
- une obligation de coopération envers les Autorités de contrôle et avec le Responsable du Traitement
- des garanties en matière de protection des données.

ARTICLE 7 : RESPONSABILITÉ

La responsabilité des Exportateurs de données peut être mise en cause devant les Autorités de contrôle compétentes et/ou devant les tribunaux compétents par la Personne concernée et par les Responsables du Traitement avec lesquels ils ont conclu un Contrat de Service en cas de non-respect des présentes BCR ou des Réglementations applicables en matière de protection des Données qui leur sont applicables.

L'Exportateur de Données assume la responsabilité des actes d'autres Entités BCR établies en dehors de l'EEE ou des violations causées par un Sous-traitant ultérieur externe établi en dehors de l'EEE et s'engage à prendre les mesures nécessaires pour y remédier et à verser une indemnisation au titre de tous dommages résultant d'une violation des BCR.

L'Exportateur de Données assumera la responsabilité de la même manière que s'il avait lui-même commis la violation dans l'État membre de l'EEE dans lequel il est basé en lieu et place de l'Entité BCR située en dehors de l'EEE ou du Sous-traitant ultérieur externe établi en dehors de l'UE. L'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.

En tout état de cause, si une Entité du Groupe LEYTON est tenue responsable d'une violation des présentes BCR commise par un Importateur de Données, l'Exportateur de Données peut demander une indemnisation à l'Entité BCR n'ayant pas respecté les BCR au titre de tous coûts, frais, dommages, dépenses ou pertes qu'il a subis.

ARTICLE 8 : RESPONSABILITÉ À L'ÉGARD DE TIERS

Article 8.1: RESPONSABILITE A L'EGARD DU RESPONSABLE DU TRAITEMENT

Le Client, agissant en qualité de Responsable du Traitement, est en droit d'exiger l'exécution des BCR par toute Entité BCR au titre des violations qu'elle a commises.

En outre, le Client a le droit d'exiger l'exécution des BCR par toute Entité BCR agissant en qualité d'Exportateur de Données en cas de :

i) manquement aux BCR ou au Contrat de Service par une Entité BCR établie en dehors de l'EEE

ii) manquement par un Sous-traitant ultérieur externe établi en dehors de l'EEE à ses obligations applicables conformément à l'Article 6.7: .

Article 8.2: RESPONSABILITE A L'EGARD DES TIERS BENEFICIAIRES

Les Personnes concernées sont en droit d'introduire une réclamation auprès :

- de toute Autorité de contrôle (en particulier l'Autorité de contrôle de l'État membre de l'EEE dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise) et
- du tribunal compétent dans l'EEE (la Personne concernée ayant le choix de saisir les tribunaux de l'État dans lequel le Responsable du Traitement ou le Sous-traitant a un établissement ou dans lequel se trouve la résidence habituelle de la Personne concernée).

En cas de violation par une Entité BCR ou un Sous-traitant ultérieur externe établi en dehors de l'EEE, les Personnes concernées peuvent engager une procédure contre l'Entité BCR en tant qu'Exportateur de Données (voir l'ARTICLE 7 : du présent document).

8.2.1. DROITS DIRECTEMENT OPPOSABLES AU SOUS-TRAITANT

Les Personnes concernées peuvent faire valoir les BCR en tant que tiers bénéficiaires directement contre le Sous-traitant si les exigences dont il est question s'appliquent expressément aux Sous-traitants en application du RGPD. À cet égard, les Personnes concernées peuvent faire valoir les éléments

suivants des BCR directement contre l'Entité BCR basée dans l'EEE exportant les données, agissant en tant que Sous-traitant :

- Obligation de mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées et obligation de notifier, dans les meilleurs délais après en avoir pris connaissance, toute violation de Données à caractère personnel au Client (Article 6.3: et 6.4) ;
- Obligation de respecter les instructions du Client en ce qui concerne le traitement de données, y compris pour les Transferts de Données vers des Pays tiers (Article 6.5:) ;
- Obligation de coopérer avec le Responsable du Traitement et de l'aider à respecter et à démontrer le respect de la législation, notamment en ce qui concerne son obligation de donner suite aux demandes dont les Personnes concernées le saisissent en vue d'exercer leurs droits (Article 6.6:) ;
- Obligation de respecter les conditions lors de l'engagement d'un Sous-traitant ultérieur, qu'il soit interne ou externe au Groupe (Article 6.7:) ;
- Droit de soumettre une réclamation par le biais des mécanismes internes de soumission de réclamations (Article 10.2:)
- Stipulations relatives à la responsabilité et à l'indemnisation (ARTICLE 7 : , Article 8.2: Article 8.2.1)
- Stipulations relatives à la compétence (Article 8.2:) ;
- Facilité d'accès aux BCR (Article 9.2:) ;
- Obligation de coopérer avec l'Autorité de Contrôle (ARTICLE 11 :) ;
- Législation nationale empêchant le respect des BCR (6.1.1, 6.6.1, 16) ;
- Droits de tiers bénéficiaires pour les Personnes concernées (Article 8.2:).

8.2.2. Droits opposables au sous-traitant lorsque la Personne concernee n'est pas en mesure d'introduire une Reclamation contre le Client agissant en qualite de Responsable du Traitement

Les Personnes concernées peuvent également exiger l'exécution des BCR en tant que tiers bénéficiaires lorsque la Personne concernée n'est pas en mesure d'introduire une réclamation contre le Client, agissant en qualité de Responsable du Traitement, en raison du fait que le Client a factuellement disparu, que son existence juridique a pris fin ou qu'il est devenu insolvable, à moins qu'une entité lui ayant succédé n'ait assumé l'intégralité des obligations légales du Responsable du Traitement par contrat ou par effet de la loi, auquel cas la Personne concernée peut faire valoir ses droits contre ladite Entité au titre des éléments suivants :

- La facilité d'accès aux BCR pour les Personnes concernées et, en particulier, la facilité d'accès aux informations concernant les droits des tiers bénéficiaires pour la Personne concernée en bénéficiant (Article 9.2: Article 9.2:)
- L'obligation de respecter les présentes BCR (Article 6.1: Article 6.1:)

- L'existence d'une procédure de gestion des réclamations pour les BCR (Article 10.2:)
- La création de droits de tiers bénéficiaires pour les Personnes concernées, y compris la possibilité d'introduire une réclamation auprès de l'Autorité de contrôle compétente et devant les tribunaux (Article 8.2:)
- La charge de la preuve incombe aux Entités BCR (Article 8.3:)
- L'obligation des Entités BCR de verser une indemnisation et de remédier aux violations des BCR (ARTICLE 7 : , Article 8.2:)
- L'obligation de coopérer avec l'Autorité de Contrôle (ARTICLE 11 :)
- L'obligation de coopérer avec le Responsable du Traitement (Article 6.6:)
- L'obligation de respecter les principes de protection des données énoncés dans le présent document (Article 6.3: , Article 6.5: , Article 6.6: , Article 6.7: , 6.8)
- Les exigences de transparence lorsque la législation nationale ne permet pas au groupe de respecter les BCR (6.1.1, 6.6.1, 16)
- La liste des entités soumises aux BCR.

L'Entité BCR n'est responsable des dommages causés par le Traitement que si elle n'a pas respecté les obligations prévues par les Réglementations applicables en matière de protection des Données qui incombent spécifiquement aux Sous-traitants ou qu'elle a agi en-dehors des instructions licites du Client, agissant en qualité de Responsable du Traitement ou des stipulations des BCR ou contrairement à celles-ci (Art. 82.2 du RGPD).

Si l'Entité BCR et le Client, agissant respectivement qualité de Sous-traitant et de Responsable du Traitement, participent au même Traitement et sont jugés responsables d'un dommage causé par ce Traitement, la Personne concernée est en droit d'obtenir une indemnisation au titre du dommage dans sa totalité directement du Sous-traitant (Art. 82.4 du RGPD).

Article 8.3: CHARGE DE LA PREUVE

Tout préjudice subi par une Personne concernée ou par un Responsable du Traitement, qui est lié à un Transfert de Données à caractère personnel réalisé dans le cadre d'un Contrat de Service est présumé avoir été causé par un manquement aux présentes BCR par l'Importateur de Données ou par un Sous-traitant ultérieur externe.

Dans ce cas, la charge de la preuve incombe à l'Exportateur de Données, qui doit prouver que l'Importateur de Données ou le Sous-traitant ultérieur externe n'est pas responsable de l'acte qui est à l'origine du préjudice invoqué par cette Personne concernée ou ce Responsable du Traitement.

ARTICLE 9 : COMMUNICATION DES BCR

Article 9.1: REFERENCE DANS LES CONTRATS DE SERVICE

Les Entités BCR doivent faire référence aux présentes BCR dans tous les Contrats de service conclus avec les Responsables du Traitement, qui devront inclure un lien hypertexte permettant d'y accéder par voie électronique. Le Contrat de Service doit mentionner le fait que les Entités BCR contribueront à des audits, y compris des inspections, menés par le Responsable du Traitement ou un autre auditeur mandaté par le Responsable du Traitement, et définir les modalités et conditions applicables à cet audit. Lesdites modalités et conditions applicables ne doivent pas porter atteinte au droit du Responsable du Traitement de réaliser l'audit.

Article 9.2: MISE A LA DISPOSITION DU PUBLIC

À compter de son approbation définitive par l'Autorité de contrôle chef de file, la version publique du présent document sera mise à disposition sur le site Internet institutionnel du Groupe Leyton et des filiales concernées et devra être facilement accessible par les Personnes concernées.

ARTICLE 10 : GOUVERNANCE EN MATIÈRE DE CONFORMITÉ

Article 10.2: INTERLOCUTEUR

Le DPO est l'interlocuteur de toutes les Entités BCR et des Personnes concernées, qui peuvent le contacter à l'adresse électronique dpo@leyton.com.

La Personne concernée peut contacter le DPO pour :

- exercer ses droits
- soumettre une réclamation relative à la confidentialité des données si la Personne concernée considère qu'une violation des Réglementations applicables en matière de protection des Données a été commise ou que les BCR ne sont pas respectées.

Si une Personne concernée soumet une réclamation ou une demande directement à une Entité BCR, le DPO informera le Responsable du Traitement de la réclamation ou de la demande conformément à la procédure définie à l'Article 6.2: et à l'Article 6.6.2 du présent document. Le DPO sera responsable uniquement de la gestion de ces demandes conformément aux instructions du Responsable du Traitement. Si le Responsable du Traitement a factuellement disparu, a cessé d'exister ou est devenu insolvable, le DPO gérera alors ces demandes directement, dans la mesure du possible.

Les demandes et/ou réclamations doivent être traitées dans les meilleurs délais et en tout état de cause dans un délai d'un mois après leur réception et le DPO

doit prendre toutes les mesures nécessaires pour régler le problème. Le délai indiqué ci-dessus peut être porté à deux mois en fonction de la complexité et du nombre de demandes. La Personne concernée doit être informée de tout retard ainsi que des motifs de ce retard.

Si le DPO considère que la demande ou la réclamation n'est pas recevable, le DPO informera la Personne concernée, dans le même délai, des raisons pour lesquelles il ne prend aucune mesure et de la possibilité d'introduire une réclamation auprès de l'Autorité de contrôle compétente et de saisir le tribunal.

Les Personnes concernées conserveront en tout état de cause le droit d'introduire une réclamation auprès d'une Autorité de contrôle ou des tribunaux compétents.

La DPO devra également gérer les demandes des Autorités de contrôle, de manière à ce qu'elles soient gérées plus efficacement au sein des Entités BCR.

ARTICLE 11 : MODIFICATION DES BCR

À l'initiative du DPO, avec le consentement du Conseil d'administration de Thésée, ou à l'initiative de ce dernier, les présentes BCR pourront être modifiées afin de prendre en compte notamment :

(i) les modifications et/ou évolutions des Réglementations applicables en matière de protection des Données ;

(ii) les modifications de la structure du Groupe Leyton.

Ces modifications des BCR ou de la liste des Entités BCR seront documentées et archivées ; les anciennes versions seront sauvegardées sous format numérique.

Dans un tel cas, les modifications deviendront opposables aux Entités BCR après leur notification aux Entités BCR et une fois que les modifications auront été communiquées à toutes les Entités BCR et aux Autorités de contrôle pertinentes via les Autorités de contrôle compétentes et que la nouvelle version aura été mise à la disposition des Personnes concernées, des Responsables du Traitement et des employés.

Les modifications des BCR seront systématiquement portées à la connaissance de toutes les entités du Groupe LEYTON, des Autorités de contrôle compétentes via la CNIL et des Responsables du Traitement par le DPO, dès que possible.

Si une modification porte sur les conditions de Traitement, les informations doivent être transmises au Responsable du Traitement en temps opportun, de manière à donner au Responsable du Traitement la possibilité d'émettre des objections à l'encontre de la modification ou de résilier le contrat avant l'application de la modification (par exemple, tout changement prévu concernant l'ajout ou le remplacement de Sous-traitants ultérieurs, avant que les données ne soient communiquées au nouveau Sous-traitant ultérieur).

ARTICLE 11 : COOPÉRATION AVEC LES AUTORITÉS DE CONTRÔLE

Les Autorités de contrôle peuvent également procéder elles-mêmes à des audits au titre de la protection des données par chaque Entité BCR. Si l'audit des Autorités de contrôle donne lieu à des observations, les Entités BCR prendront en compte ces observations et mettront en œuvre des mesures correctives sur demande.

Chaque Entité BCR s'engage à coopérer avec les Autorités de contrôle compétentes à l'égard des Responsables du Traitement au nom et pour le compte desquels elle traite les Données. Les Autorités de contrôle peuvent procéder à des vérifications au titre de chaque Entité BCR. Les Entités BCR doivent prendre en compte les recommandations des Autorités de contrôle et se conformer à leurs décisions, sans aucune limitation.

ARTICLE 12 : LES OUTILS POUR LA CONFORMITE

Afin d'aider le Personnel des Entités BCR à appliquer les présentes BCR et les règles résultant des Réglementations, des politiques connexes seront mises en œuvre concernant :
(i) la conservation des données et le système d'archivage ;
(ii) la gestion des Violations de Données à caractère personnel ;
(iii) la gestion des droits de la Personne concernée ;
(iv) la Protection de Données
(v) l'utilisation des systèmes informatiques et de communication.

ANNEXE 1 : LISTE ET PRESENTATION DES ENTITES S'ETANT ENGAGEES A RESPECTER LES BCR

Leyton est un Groupe international dont les expertises s'articulent autour de 3 métiers : le financement de l'innovation, le conseil et les services externalisés. Le Groupe Leyton est présent dans douze (12) pays, parmi lesquels figurent un (1) Pays Tiers (Maroc), huit (8) Etats Membres (France, Belgique, Espagne, Portugal, Italie, Allemagne, Pologne, Suède et Pays-Bas), et deux (2) pays reconnus comme garantissant partiellement un niveau de protection des Données (Canada, Royaume Uni).

THESEE
16 Boulevard Garibaldi
92130 Issy les Moulineaux
SIREN : 491828554

Thésée est la société holding de Leyton Group.

LEYTON FRANCE
16 Boulevard Garibaldi
92130 Issy les Moulineaux
SIREN : 504868399

Leyton France est un prestataire de service qui traite des données pour l'ensemble des finalités décrites dans l'article 5.2 de ce document. Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON CTR
16 Boulevard Garibaldi
92130 Issy les Moulineaux
SIREN : 414600270

CTR est un prestataire de service qui traite des données pour l'ensemble des finalités décrites dans l'article 5.2 de ce document. Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

OAP
16 Boulevard Garibaldi
92130 Issy les Moulineaux
SIREN : 523311058

OAP est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- l'optimisation de l'allocation des ressources de l'entreprise (Télécom, Flotte automobile, intérim, dépenses énergie, assurances etc.)

- l'optimisation des charges locatives
- l'analyse et le suivi du processus de facturation et des actions de recouvrement.

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

OFEE
16 Boulevard Garibaldi
92130 Issy les Moulineaux
SIREN : 504668377

OFEE est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- la livraison de Certificat d'économie d'énergie (« CEE ») ou autre dispositif national de certificats blancs;
- l'optimisation de la fiscalité de l'énergie
- l'optimisation de l'allocation des ressources de l'entreprise (dépenses énergie)

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON RISK MANAGEMENT
16 Boulevard Garibaldi
92130 Issy les Moulineaux
SIREN : 423812254

LEYTON RISK MANAGEMENT est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par l'optimisation de l'allocation des ressources de l'entreprise (assurances).
Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON JUDO
16 Boulevard Garibaldi
92130 Issy les Moulineaux
SIREN : 879286003

LEYTON BENELUX
Chaussée de la Hulpe 166
1170 Brussels
Numéro d'identification : BE0811.483.88

Leyton Belgium est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions;
- l'optimisation des charges sociales

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON NETHERLANDS
Secoya Papendorpseweg 99
3528 BJ Utrecht

Leyton Netherlands est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions;
- l'optimisation des charges sociales

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON IBERIA
Plaza Xavier Cugat 2, Edificio D, 4 Planta
08017 Sant Cugat del Vallés, Barcelona.
Numéro d'identification : B-66286188

Leyton IBERIA est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions;
- l'optimisation de la fiscalité locale et nationale ;
- l'optimisation des charges sociales

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

THESEE PORTUGAL
R. Daciano Baptista Marques, 245. Lake Towers – Edificio D
4400-617 Vila Nova de Gaia (Porto)

Thésée PORTUGAL est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions.

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON ITALIA
Via Melchiorre Gioia 26
20124 Milano
Numéro d'identification : REA MI 2119395
Leyton Italia est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions;
- la livraison de Certificat d'économie d'énergie (« CEE ») ou autre dispositif national de certificats blancs;
- l'optimisation de la fiscalité de l'énergie ;
- l'optimisation de l'allocation des ressources de l'entreprise (dépenses énergie)
- l'optimisation de la fiscalité locale et nationale ;

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

OFEE ITALIA
Via Melchiorre Gioia 26
20124 Milano
Numéro d'identification : REA MI 2534436

OFEE Italia est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- la livraison de Certificat d'économie d'énergie (« CEE ») ou autre dispositif national de certificats blancs;
- l'optimisation de la fiscalité de l'énergie
- l'optimisation de l'allocation des ressources de l'entreprise (dépenses énergie)

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON POLAND
Wspólna 70
00-687 Warszawa
Numéro d'identification : KRS 0000739425

Leyton Poland est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par Les

dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions.
Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON GERMANY
Bleichstraße 20
40211 Düsseldorf - Germany
Numéro d'identification : HRB: 89458

Leyton Germany est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions.
Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON SWEDEN
Klarabergsviadukten 63,
11164 Stockholm
Numéro d'identification : 559272 – 2663

Leyton Sweden est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions.
Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON MAROC
Plateau 502, 5ème étage Park Shore
14 Parc Casanearshore Sidi Maârouf Casablanca
Numéro d'identification : 165799

Leyton Maroc est une société de service faisant partie du Groupe Leyton et agissant comme sous-traitant ultérieur pour les entités du Groupe Leyton dans le cadre des traitements dont les finalités sont décrites précédemment (§ " Article 5.2: FINALITES).

THESEE MAROC
Plateau 502, 5ème étage Park Shore
14 Parc Casanearshore Sidi Maârouf Casablanca
Numéro d'identification : 245533

THESEE Maroc est une société de service faisant partie du Groupe Leyton et agissant comme sous-traitant ultérieur pour les entités du Groupe Leyton dans

le cadre des traitements dont les finalités sont décrites précédemment (§ " Article 5.2: FINALITES).

THESEE CANADA
1260 Boulevard Robert Bourassa
Montreal, Quebec H3B 3B9
Numéro d'identification : 1165640989

Thésée Canada est la société holding de Leyton Finder Expert.

LEYTON FINDER EXPERT
1260 Boulevard Robert Bourassa
Montreal, Quebec H3B 3B9
Numéro d'identification : 1146449062

Leyton Finder Expert est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions.
Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

LEYTON UNITED KINGDOM
Harmsworth House
13-15 Bouverie Street
EC4Y 8DP, London

Leyton United Kingdom est un prestataire de service qui traite des données pour l'ensemble ou partie des finalité(s) suivante(s) : l'accompagnement en matière d'économies ou de leviers de financements générés notamment par

- Les dispositifs d'incitations fiscales à la recherche et l'innovation, le Crédit Impôt Recherche (« CIR ») et les aides et subventions;
- l'optimisation des charges sociales;
- la livraison de Certificat d'économie d'énergie (« CEE ») ou autre dispositif national de certificats blancs;
- l'optimisation de la fiscalité de l'énergie ;
- l'optimisation de l'allocation des ressources de l'entreprise (dépenses énergie).

Ses clients sont exclusivement des personnes morales de droit public et de droit privé.

ANNEXE 2: ARTICLES DU RGPD MENTIONNES DANS LES BCR

ART. 28. RGPD SOUS-TRAITANT

1. Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.

2. Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

3. Le traitement par un sous-traitant est régi par 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, définit 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. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant:

   a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, 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 juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;

   b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité;

   c) prend toutes les mesures requises en vertu de l'article 32;

   d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant;

e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III;

f) aide 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;

g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel; et

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article 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 contribuer à ces audits.

En ce qui concerne le point h) du premier alinéa, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

4. Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, 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 aux exigences du présent règlement. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

5. L'application, par un sous-traitant, d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer l'existence des

garanties suffisantes conformément aux paragraphes 1 et 4 du présent article.

6. Sans préjudice d'un contrat particulier entre le responsable du traitement et le sous-traitant, le contrat ou l'autre acte juridique visé aux paragraphes 3 et 4 du présent article peut être fondé, en tout ou en partie, sur les clauses contractuelles types visées aux paragraphes 7 et 8 du présent article, y compris lorsqu'elles font partie d'une certification délivrée au responsable du traitement ou au sous-traitant en vertu des articles 42 et 43.

7. La Commission peut établir des clauses contractuelles types pour les questions visées aux paragraphes 3 et 4 du présent article et conformément à la procédure d'examen visée à l'article 93, paragraphe 2.

8. Une autorité de contrôle peut adopter des clauses contractuelles types pour les questions visées aux paragraphes 3 et 4 du présent article et conformément au mécanisme de contrôle de la cohérence visé à l'article 63.

9. Le contrat ou l'autre acte juridique visé aux paragraphes 3 et 4 se présente sous une forme écrite, y compris en format électronique.

10. Sans préjudice des articles 82, 83 et 84, si, en violation du présent règlement, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement.

ART. 29 RGPD TRAITEMENT EFFECTUE SOUS L'AUTORITE DU RESPONSABLE DU TRAITEMENT OU DU SOUS-TRAITANT

Le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre.

ART. 30 RGPD REGISTRE DES ACTIVITES DE TRAITEMENT

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.

5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

ART. 32 RGPD SÉCURITÉ DU TRAITEMENT

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

    a) la pseudonymisation et le chiffrement des données à caractère personnel;

    b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

    c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

    d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une

autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

ART. 33 RGPD NOTIFICATION A L'AUTORITE DE CONTROLE D'UNE VIOLATION DE DONNEES A CARACTERE PERSONNEL

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins:

   a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

   b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

ART. 34 RGPD COMMUNICATION A LA PERSONNE CONCERNEE D'UNE VIOLATION DE DONNEES A CARACTERE PERSONNEL

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes

concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

ART. 35 RGPD ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES

1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2. Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

3. L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants:

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

4. L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

5. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

6. Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

7. L'analyse contient au moins:

   a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;

   b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

   c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et

   d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

ART. 36 RGPD CONSULTATION PREALABLE

1. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'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.

2. Lorsque l'autorité de contrôle est d'avis que le traitement envisagé visé au paragraphe 1, constituerait une violation du présent règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage des pouvoirs visés à l'article 58. Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement envisagé. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.

3. Lorsque le responsable du traitement consulte l'autorité de contrôle en application du paragraphe 1, il lui communique:

   a) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises;

   b) les finalités et les moyens du traitement envisagé;

   c) les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du présent règlement;

   d) le cas échéant, les coordonnées du délégué à la protection des données;

   e) l'analyse d'impact relative à la protection des données prévue à l'article 35; et

   f) toute autre information que l'autorité de contrôle demande.

4. Les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.

5. Nonobstant le paragraphe 1, le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique.

ART. 37 RGPD DESIGNATION DU DELEGUE A LA PROTECTION DES DONNEES

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

   a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

   b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature,

de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

2. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

3. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

4. Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

5. Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.

6. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

7. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

ART. 45 RGPD TRANSFERTS FONDES SUR UNE DECISION D'ADEQUATION

1. Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

2. Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte, en particulier, des éléments suivants:

   a) l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées;

   b) l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres; et

   c) les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2 du présent article. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de

l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, nomme la ou des autorités de contrôle visées au paragraphe 2, point b), du présent article. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

4. La Commission suit, de manière permanente, les évolutions dans les pays tiers et au sein des organisations internationales qui pourraient porter atteinte au fonctionnement des décisions adoptées en vertu du paragraphe 3 du présent article et des décisions adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE.

5. Lorsque les informations disponibles révèlent, en particulier à l'issue de l'examen visé au paragraphe 3 du présent article, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale n'assure plus un niveau de protection adéquat au sens du paragraphe 2 du présent article, la Commission si nécessaire, abroge, modifie ou suspend la décision visée au paragraphe 3 du présent article par voie d'actes d'exécution sans effet rétroactif. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

6. Pour des raisons d'urgence impérieuses dûment justifiées, la Commission adopte des actes d'exécution immédiatement applicables en conformité avec la procédure visée à l'article 93, paragraphe 3.

7. La Commission engage des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation donnant lieu à la décision adoptée en vertu du paragraphe 5.

8. Une décision adoptée en vertu du paragraphe 5 du présent article est sans préjudice des transferts de données à caractère personnel vers le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou à l'organisation internationale en question, effectués en application des articles 46 à 49.

9. La Commission publie au Journal officiel de l'Union européenne et sur son site internet une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.

10. Les décisions adoptées par la Commission sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission adoptée conformément au paragraphe 3 ou 5 du présent article.

ART. 46 RGPD TRANSFERTS MOYENNANT DES GARANTIES APPROPRIEES

1. En l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par:

   a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics;

   b) des règles d'entreprise contraignantes conformément à l'article 47;

   c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;

   d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;

   e) un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées; ou

   f) un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

3. Sous réserve de l'autorisation de l'autorité de contrôle compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, par:

   a) des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le

destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale; ou

b) des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

4. L'autorité de contrôle applique le mécanisme de contrôle de la cohérence visé à l'article 63 dans les cas visés au paragraphe 3 du présent article.

5. Les autorisations accordées par un État membre ou 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 décisions adoptées par la Commission sur le fondement de l'article 26, paragraphe 4, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par une décision de la Commission adoptée conformément au paragraphe 2 du présent article.

ART. 47 RGPD RÈGLES D'ENTREPRISE CONTRAIGNANTES

1. L'autorité de contrôle compétente approuve des règles d'entreprise contraignantes conformément au mécanisme de contrôle de la cohérence prévu à l'article 63, à condition que:

a) ces règles soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés;

b) elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel; et

c) elles répondent aux exigences prévues au paragraphe 2.

2. Les règles d'entreprise contraignantes visées au paragraphe 1 précisent au moins:

a) 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;

b) 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 en question;

c) leur nature juridiquement contraignante, tant interne qu'externe;

d) l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes;

e) les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l'article 22, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément à l'article 79 et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes;

f) l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause;

g) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f) du présent paragraphe sont fournies aux personnes concernées, en sus des informations visées aux articles 13 et 14;

h) les missions de tout délégué à la protection des données, désigné conformément à l'article 37, ou de toute autre personne ou entité chargée de la surveillance du respect des règles d'entreprise contraignantes au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations;

i) les procédures de réclamation;

j) les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués à la personne ou à l'entité visée au point h) et au conseil d'administration de l'entreprise qui exerce le contrôle du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, et devraient être mis à la disposition de l'autorité de contrôle compétente sur demande;

k) les mécanismes mis en place pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle;

l) le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures visés au point j);

m) les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, est soumise dans un pays tiers qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les règles d'entreprise contraignantes; et

n) la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel.

3. La Commission peut, pour les règles d'entreprise contraignantes au sens du présent article, préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

ART. 49 RGPD DEROGATIONS POUR DES SITUATIONS PARTICULIERES

1. En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes:

   a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées;

   b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée;

   c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale;

   d) le transfert est nécessaire pour des motifs importants d'intérêt public;

   e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice;

   f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

   g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce.

   Lorsqu'un transfert ne peut pas être fondé sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières visées au premier alinéa du présent paragraphe n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt pas de

caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

2. Un transfert effectué en vertu du paragraphe 1, premier alinéa, point g), ne porte pas sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes justifiant d'un intérêt légitime, le transfert n'est effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

3. Les points a), b), et c) du premier alinéa du paragraphe 1 et le deuxième alinéa du paragraphe 1 ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

4. L'intérêt public visé au paragraphe 1, premier alinéa, point d), est reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis.

5. En l'absence de décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale. Les États membres notifient de telles dispositions à la Commission.

6. Le responsable du traitement ou le sous-traitant documente, dans les registres visés à l'article 30, l'évaluation ainsi que les garanties appropriées visées au paragraphe 1, deuxième alinéa, du présent article.

ART. 82 RGPD DROIT A REPARATION ET RESPONSABILITE

1. Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.
2. Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté

les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

4. Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

5. Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2.

6. Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant les juridictions compétentes en vertu du droit de l'État membre visé à l'article 79, paragraphe 2.

ANNEXE 3: DESCRIPTION DES MESURES DE SECURITE

1. SECURITE PHYSIQUE
- Gestion des accès par badge avec journalisation ou agents de sécurité

2. GESTION DES ACCES
- Revue annuelle des droits d'accès
- Log des modifications de permissions (GPO)
- Log des modifications de permissions serveur de fichier et domaine

3. HEBERGEMENT DES DONNES
- Data centers situés en France, certifié ISO 27001, SOC 2 Part II

4. SECURITE RESEAU
- Prévention d'intrusion avec alerte (IPS)
- Protection anti programmes malveillants
- Pare feu et inspection SSL
- Antivirus EDR
- SOC

5. REPORTING RESEAU
- Logs du trafic réseau et de sécurité
- Logs des connexions, déconnexions et activités des utilisateurs
- Supervision des applications critiques telles qu'Active Directory, SQL ou application interne

6. SECURISATION DES ORDINATEURS
- Politique de mot de passe complexe avec changement réguliers
- Blocage automatique des ordinateurs en cas d'inactivité prolongée
- Procédure de prise en main à distance sécurisée
- Mise au rebut sécurisée des disques durs

7. SECURITE DES FLUX
- VPN SSL
- Wifi WPA 2
- Anti-spam
- DKIM et DMARC
- Chiffrage des emails TLS 1.2

8. SENSIBILISATION
- Utilisation de broyeurs à papier
- Clean desk policy
- Charte d'utilisation des systèmes d'information
- Procédures internes
- Formation à la protection des données et à la sécurité