# Accord relatif au traitement de données à caractère personnel

Le présent Accord (l'« **Accord** ») est conclu entre :

(1) [Filiale de Getlink concernée], une société immatriculée au RCS de [●] sous le [●], dont l'adresse principale est sise [●], (le « **Client** »)

et

(2) [Raison sociale du Fournisseur], une société de droit [●] immatriculée sous le numéro [●] et dont le siège social est sis [●] (le « **Fournisseur** »).

Considérant que :

(A) Le présent Accord complète tout autre accord distinct passé entre les parties en vue de la fourniture des services [●] (les « **Services** ») et introduit de nouvelles dispositions visant à assurer la protection et la sécurité des données à caractère personnel par le Fournisseur dans le cadre de la fourniture des Services.

(B) Le présent Accord a pour objet de veiller à ce que le Client et le Fournisseur exécutent leurs obligations respectives en vertu de la Législation en vigueur sur la protection des données (telles que définies ci-dessous).

Définitions :

Aux fins du présent Accord, y compris les considérants ci-dessus, et sauf si le contexte en exige autrement :

« **Législation sur la protection des données** » désigne les Directives européennes 95/46/CE et 2002/58/CE, ainsi que toute législation et/ou réglementation visant leur application ou adoptée en vertu de celles-ci, ou qui modifie, remplace, réadopte ou consolide une quelconque d'entre elles, y compris le Règlement Général sur la Protection des Données 2016/679 du 27 avril 2016, et toutes les lois applicables en matière de traitement de données à caractère personnel et de confidentialité dans tout territoire concerné, y compris, le cas échéant, les directives et codes de pratique institués par les autorités de contrôle ;

« **responsable du traitement** », « **sous-traitant** », « **personne concernée** », « **données à caractère personnel** », « **traitement** » et « **mesures techniques et organisationnelles appropriées** » ont le sens qui leur est attribué aux termes de la Législation sur la protection des données ; et

« **Violation de données à caractère personnel** » désigne toute destruction, perte, altération, divulgation ou consultation accidentelle, non autorisée ou illégale des données à caractère personnel traitées par le Fournisseur dans le cadre de la fourniture des Services.

## 1. Dispositions générales

1.1 Le Fournisseur reconnaît que les dispositions du présent Accord s'appliquent aux données à caractère personnel qu'il est appelé à traiter dans le cadre de la fourniture des Services. Les activités de traitement sont décrites à l'Annexe 2.

1.2 Le Fournisseur reconnaît qu'il est le sous-traitant et que le Client est le responsable du traitement en ce qui concerne les données à caractère personnel que le Fournisseur est appelé à traiter dans le cadre de la fourniture des Services.

1.3 Le traitement s'étendra sur [indiquer la durée du traitement].

## 2. Obligations du Fournisseur

2.1 Lorsque le Fournisseur est appelé à traiter des données à caractère personnel dans le cadre de la fourniture des Services, il devra :

2.1.1 traiter lesdites données uniquement en conformité avec les instructions écrites du Client (qui peuvent être spécifiques ou de nature générale, tel qu'énoncé dans l'Accord ou autrement communiqué au Fournisseur par le Client à tout moment). Si le Fournisseur est tenu de traiter les données à caractère personnel à d'autres fins en vertu de dispositions légales de l'Union Européenne ou d'un État membre auxquelles il est soumis, il devra d'abord notifier cette exigence au Client, sauf si les dispositions légales en question le lui interdisent pour des motifs impérieux de sauvegarde de l'intérêt public ;

2.1.2 informer le Client dans les plus brefs délais s'il estime qu'une instruction relative au traitement des données à caractère personnel, donnée par le Client, enfreint la Législation en vigueur sur la protection des données ;

2.1.3 en cas de plainte ou de notifications directement ou indirectement liées au traitement des données à caractère personnel ou à la conformité de quelque partie à la Législation sur la protection des données, informer sans délai le Client et offrir, sans frais, son entière coopération et assistance concernant la plainte ou les notifications en question ;

2.1.4 apporter son aide au Client, en fonction de la nature du traitement :

2.1.4.1 afin d'assurer le respect des obligations prévues aux articles 32 à 36 du Règlement Général sur la Protection des Données, en tenant compte des informations dont dispose le Fournisseur ; et

2.1.4.2 en mettant à la disposition du Client toutes les informations que ce dernier pourrait raisonnablement demander dans le but de prouver sa conformité aux exigences de l'article 28 du Règlement général sur la protection des données en matière de désignation des sous-traitants.

Le Fournisseur ne doit pas facturer son assistance, notamment si celle-ci est rendue nécessaire et en lien direct avec un acte ou omission imputable à ce dernier, auquel cas l'assistance sera fournie à ses frais ;

2.1.5 mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées pour prévenir tout traitement non autorisé ou illégal et toute perte, destruction, altération, divulgation ou tout dommage, vol accidentels des données à caractère personnel. Ces mesures doivent être à la mesure du préjudice qui pourrait découler de tout traitement illégal, de toute perte, destruction, toute altération ou vol accidentels des données à caractère personnel et doivent prendre en compte la nature des données qui doivent être protégées. Au minimum, cette protection doit englober les exigences énoncées à l'Annexe 1 du présent Accord ;

2.1.6 si le Client en fait la demande, fournir à celui-ci une copie de toutes les données à caractère personnel dont dispose le Fournisseur, suivant le format et sur le support raisonnablement spécifié ;

2.1.7 à la fin des Services et à la demande du Client, modifier, détruire ou retourner de manière sécurisée les données à caractère personnel au Client, et supprimer les copies existantes, sauf si les dispositions légales de l'Union Européenne ou d'un État membre exigent la conservation de ces données à caractère personnel ; et

2.2 En cas de soupçons d'une Violation de données à caractère personnel, le Fournisseur doit :

2.2.1 immédiatement prendre des mesures, à ses frais, pour enquêter sur l'éventuelle Violation de données à caractère personnel afin d'identifier, prévenir et atténuer les effets de celle-ci et d'y remédier ;

2.2.2 notifier sans délai le Client aussitôt qu'il a une raison valable de croire qu'une Violation de données à caractère personnel a été commise, et lui fournir une description détaillée de ladite Violation, notamment :

2.2.2.1 l'impact probable de la Violation de données à caractère personnel ;

2.2.2.2 les catégories et une estimation du nombre de personnes concernées affectées et leurs pays de résidence, ainsi que les catégories et une estimation du nombre de données affectées ;

2.2.2.3 le risque que représente la Violation de données à caractère personnel pour les personnes physiques ; et

2.2.2.4 les mesures prises ou envisagées par le Fournisseur pour remédier à la Violation de données à caractère personnel et atténuer ses effets néfastes.

Le Fournisseur doit également fournir des mises à jour ponctuelles concernant ces informations et tout autre renseignement que le Client pourrait raisonnablement demander concernant la Violation de données à caractère personnel ; et

2.2.3 s'abstenir de divulguer ou de publier tout fichier, communication, notification, communiqué de presse ou rapport concernant la Violation de données à caractère personnel sans le consentement écrit préalable du Client (sauf si la loi l'y oblige).

2.3 En outre, le Fournisseur doit :

2.3.1 s'abstenir de transférer ou d'autoriser l'accès aux données à caractère personnel à des tiers [(y compris les sociétés affiliées, les sociétés apparentées ou les sous-traitants)] sans l'accord écrit préalable du Client. Au cas où le Client autorise le Fournisseur à engager des tiers pour fournir une partie des Services, le Fournisseur doit inclure dans tout contrat passé avec les tiers en question des dispositions en faveur du Client qui soient égales aux présentes et respectent les exigences de la Législation en vigueur sur la protection des données. Afin de lever toute équivoque, au cas où un tiers manque à ses obligations en vertu d'un contrat de sous-traitant ou de toute Législation en vigueur sur la protection des données, le Fournisseur demeurera entièrement responsable envers le Client de l'exécution de ses obligations prévues aux termes des présentes ;

2.3.2 s'assurer que l'accès aux données à caractère personnel se limite aux employés, mandataires ou sous-traitants qui ont besoin d'y accéder pour exécuter les obligations du Fournisseur en vertu du présent Accord ;

2.3.3 veiller à ce que les personnes qui doivent accéder aux données à caractère personnel soient bien informées de leurs obligations en matière de sécurité et de protection desdites données et exiger de celles-ci la prise d'engagements contraignants, comprenant notamment une obligation de confidentialité concernant les données à caractère personnel, de manière à maintenir les niveaux de sécurité et de protection prévus aux termes du présent Accord ; et

2.3.4 s'abstenir de divulguer les données à caractère personnel, que ce soit de manière directe ou indirecte, à quelque personne, cabinet ou société que ce soit, sauf si (i) la loi l'exige ou si (ii) le Client l'y enjoint par écrit, exception faite de ceux de ses employés, mandataires et sous-traitants impliqués dans le traitement des données à caractère personnel et liés par les engagements contraignants visés à la clause 2.3.3.

## 3. Droit de vérification du Client

3.1 Le Client et ses auditeurs ou mandataires autorisés ont le droit d'effectuer des audits ou des contrôles moyennant un préavis raisonnable pendant la durée de l'Accord [et pour une période de [12] mois après son expiration], lesquels supposent l'accès aux et l'inspection des locaux, équipements, documents, données électroniques et employés du Fournisseur et des sous-traitants qui sont mis à contribution aux fins de la fourniture des Services. Le Fournisseur est tenu d'apporter toute assistance raisonnable afin d'aider le Client à exercer

son droit de vérification en vertu du présent paragraphe. La finalité d'un audit en vertu de la présente clause est de vérifier que le Fournisseur traite les données à caractère personnel conformément à ses obligations en vertu des présentes.

3.2 L'exigence de donner un préavis conformément à la clause 3.1 ne s'appliquera pas si le Client est convaincu que le Fournisseur a manqué à ses obligations aux termes du présent Accord.

4. **Mécanismes de transfert**

4.1 Le Fournisseur doit s'abstenir de transférer les données à caractère personnel en dehors de l'Espace économique européen ou vers tout pays à l'égard duquel la Commission européenne n'a pas rendu une décision valable relative à l'adéquation du niveau de protection des données, sauf avec l'accord écrit préalable du Client.

5. **Garanties**

5.1 Le Fournisseur s'engage à :

5.1.1 traiter les données à caractère personnel dans le respect de l'ensemble des lois, actes, règlements, ordonnances, normes et autres instruments similaires applicables, y compris, notamment, la Législation sur la protection des données ; et

5.1.2 faire tout ce qui est en son pouvoir pour protéger les données à caractère personnel de tout traitement non autorisé ou illégal et de toute perte, destruction ou toute altération accidentels, et confirme qu'il a mis en œuvre les mesures techniques et organisationnelles indiquées à l'Annexe 1 afin de prévenir tout traitement non autorisé ou illégal et toute perte, destruction ou toute altération accidentels des données à caractère personnel.

6. **Responsabilité**

6.1 Le Fournisseur est responsable. Il est tenu d'indemniser le Client eu égard à quelque action, procédure, obligation, frais, réclamation, perte, dépense et demande visant ce dernier et découlant :

- directement ou en étant en lien avec des activités de traitement de données menées par le Fournisseurs ;
- découlant notamment de toute demande, réclamation ou action de tiers, violation contractuelle, négligence, fraude, faute intentionnelle, violation d'obligation légale ou inobservation de la Législation sur la protection des données par le Fournisseur ou ses employés, mandataires ou sous-traitants.

6.2 La responsabilité du Fournisseur visée à la clause 6.1 ne peut excéder la somme de 10 millions d’euros ou la limite supérieure de la couverture d'assurance de ce dernier, selon l'éventualité la plus élevée. Afin de lever toute équivoque, les limites de responsabilité

visées aux termes de la présente clause 6.2 s'appliquent par événement et non dans l'ensemble.

7. **Compétence**

7.1 Les présentes clauses et tout litige ou réclamation (même non contractuel) découlant de, ou se rapportant à l'objet ou à la formation du présent Accord sont régis et interprétés conformément à la loi française.

7.2 Le Fournisseur et le Client se soumettent irrévocablement à la compétence exclusive des tribunaux français pour régler tout litige ou réclamation (y compris les litiges ou les réclamations non contractuels) découlant de, ou se rapportant à l'Accord, son objet ou sa formation.

| | |
|---|---|
| Signé au nom et pour le compte de [Filiale de Getlink concernée]<br><br>Nom :<br><br>Fonction :<br><br>Date :<br><br>Signature : | Signé au nom et pour le compte de [Insérer le Nom]<br><br>Nom :<br><br>Fonction :<br><br>Date :<br><br>Signature : |

## Annexe 1

## Mesures de sécurité

### 1. Contrôle d'accès aux locaux et aux installations

Des précautions doivent être prises pour prévenir tout accès physique non autorisé aux locaux et aux installations où sont conservées les données à caractère personnel. Ces précautions englobent les éléments suivants :

- Système de contrôle d'accès
- Lecteur de carte d'identification, carte magnétique, carte à puce
- (Création de) codes secrets
- Fermeture de portes (portes avec ouverture électrique, etc.)
- Surveillance des installations
- Système d'alarme, vidéosurveillance
- Enregistrement des entrées et sorties dans les installations

### 2. Contrôle d'accès aux systèmes

Des précautions doivent être prises pour prévenir tout accès non autorisé aux systèmes informatiques. Ces précautions englobent les mesures techniques et organisationnelles suivantes visant l'identification et l'authentification des utilisateurs :

- Procédures relatives aux mots de passe (notamment les caractères spéciaux, la longueur minimale, l'exigence de changement de mot de passe)
- Aucun accès pour les visiteurs ou les comptes anonymes
- Gestion centralisée de l'accès aux systèmes
- Accès aux systèmes informatiques soumis à l'approbation de la direction des RH et des administrateurs système

### 3. Contrôle d'accès aux données

Des précautions doivent être prises pour éviter que les utilisateurs autorisés accèdent à des données qui dépassent le cadre de leurs droits d'accès ainsi que pour prévenir toute [saisie, lecture, copie, suppression] modification ou divulgation non autorisée des données. Ces précautions englobent les éléments suivants :

- Catégorisation des droits d'accès
- Définition des droits d'accès en fonction des responsabilités
- Enregistrement automatisé des accès d'utilisateurs grâce aux systèmes informatiques
- Prise de précautions pour prévenir l'utilisation de systèmes de traitement automatisé de données par des personnes non autorisées, à l'aide d'équipements de transmission de données

**4. Contrôle de divulgation**

Des précautions doivent être prises pour prévenir tout accès non autorisé, altération ou suppression de données pendant le transfert, et pour s'assurer que tous les transferts sont sécurisés et qu'une trace de ceux-ci est conservée. Ces précautions englobent les éléments suivants :

- Utilisation obligatoire d'un réseau privé exclusif pour tous les transferts de données
- Chiffrement à l'aide d'un Réseau Privé Virtuel (VPN) pour les accès à distance, le transport et la communication des données.
- Interdiction des supports amovibles
- Création d'une piste de vérification de tous les transferts de données

**5. Contrôle de saisie**

Des précautions doivent être prises pour s'assurer que toutes les activités de gestion et de maintenance des données sont consignées, et une piste de vérification doit être créée afin de savoir si des données ont été saisies, modifiées ou supprimées et par qui.

Ces précautions englobent les éléments suivants :

- Garder des traces des activités menées sur les systèmes informatiques
- S'assurer qu'il est possible de vérifier et de déterminer à quels organismes les données à caractère personnel ont été ou pourraient être transmises ou rendues disponibles à l'aide d'équipement de transmission de données
- S'assurer qu'il est possible de vérifier et de déterminer le type de données à caractère personnel saisies dans les systèmes de traitement automatisé de données, ainsi que le moment et l'auteur de la saisie ;

**6. Contrôle de la conformité du traitement aux instructions**

Des mesures doivent être mises en place pour s'assurer que les données sont traitées de manière strictement conforme aux instructions de l'importateur de données. Ces mesures englobent les éléments suivants :

- Formulation sans ambiguïté des instructions contractuelles
- Suivi de l'exécution des contrats

**7. Contrôle de disponibilité**

Des précautions doivent être prises pour assurer la protection des données contre toute destruction ou perte accidentelle.

Ces mesures englobent les éléments suivants :

- S'assurer que les systèmes installés peuvent, en cas d'interruption, être rétablis
- S'assurer que les systèmes fonctionnent et que les failles sont signalées
- S'assurer que les données à caractère personnel conservées ne peuvent pas être endommagées en raison d'une défaillance du système
- Alimentation sans interruption (ASI)
- Procédures de continuité de l'activité
- Stockage à distance
- Antivirus/pare-feu

**8. Contrôle de la séparation**

Des mesures doivent être prises afin que les données collectées à des fins distinctes soient traitées séparément.

Ces mesures englobent les éléments suivants :

- Restriction de l'accès aux données stockées à différentes fins en fonction des responsabilités des membres du personnel.
- Séparation des systèmes informatiques de l'activité
- Séparation des environnements d'essai et de production informatiques

**9.** Les mesures de sécurité exigées si le Fournisseur intègre son système informatique à celui d'Eurotunnel.

## Annexe 2

## Description des activités de traitement

**Personnes concernées**

Les données à caractère personnel visent les catégories de personnes concernées suivantes :

[●] *[Exemple : le personnel du Client ou toutes autres personnes travaillant pour ce dernier (y compris les employés ou les temporaires et contractuels), les clients passagers]*

**Catégories de données**

Les données à caractère personnel transférées visent les catégories de données suivantes :

[●] *[Exemple : les informations d'identification : nom (et noms antérieurs), coordonnées, date de naissance, historique des adresses, pays de résidence, données financières et coordonnées bancaires.]*

**Catégories particulières de données (le cas échéant)**

Les données à caractère personnel transférées visent les catégories particulières de données suivantes :

[●] *[Exemple : État de santé justifiant l'administration d'un régime de prestation d'invalidité ou médicale à long terme, dossiers médicaux, rapports de rendement ou de travail/ajustement et rapports d'accidents professionnels]*

**Activités de traitement**

Les données à caractère personnel transférées seront soumises aux activités de traitement basique suivantes :

[●] *[Exemple : aux fins de la fourniture des services [●] au Client par le Fournisseur et aux fins connexes]*

# Directives sur les transferts internationaux de données conformément au Règlement général sur la protection des données

**Scénario 1**


| Transferts autorisés ? | Vers quels pays ? |
|---|---|
| **Oui** | • Membres de l'UE : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suède, République tchèque, Royaume-Uni (jusqu'au Brexit).<br>• Pays non membre de l'UE : Islande, Liechtenstein, Norvège. |

**Explication :** Si le Fournisseur est établi dans, ou transfère des données vers, un quelconque de ces pays, le modèle d'accord entre le Client (c.-à-d. Eurotunnel) et le Fournisseur n'a pas besoin d'être modifié en ce qui concerne la disposition sur le transfert des données visée à la clause 4.1 de l'Accord.

**Scénario 2**

Pays ayant *un « niveau de protection adéquat »*

| Transferts autorisés ? | Vers quels pays ? |
|---|---|
| **Oui** | • Andorre, Argentine, Canada (organisations privées qui utilisent les données à des fins d'activités commerciales), Guernesey, Île de Man, Îles Féroé, Israël, Jersey, Nouvelle-Zélande, Suisse. |

**Explication :** Si le Fournisseur est établi dans, ou transfère des données vers, un quelconque de ces pays, le modèle d'accord entre le Client (c.-à-d. Eurotunnel) et le Fournisseur n'a pas besoin d'être modifié en ce qui concerne la disposition sur le transfert des données visée à la clause 4.1 de l'Accord.

**Scénario 3**

Pays n'ayant pas *un « niveau de protection adéquat »*

| Transfert autorisé ? | Vers quels pays ? |
|---|---|
| Mesures nécessaires | • Tous les pays n'ayant pas un niveau de protection adéquat. |

**Explication :** Si le Fournisseur est basé dans, ou entend transférer des données vers, un pays en dehors de ceux cités ci-dessus, l'Accord entre le Client (c.-à-d. Eurotunnel) et le Fournisseur devra :

- intégrer par renvoi un des mécanismes de transfert de données approuvés aux termes du RGPD ; ou

- invoquer l'une des dérogations en matière de transfert de données prévues par le RGPD (notamment le consentement, la nécessité contractuelle, la défense ou l'exercice d'un droit dans le cadre d'un recours judiciaire, ou la protection des intérêts vitaux des personnes concernées). NB : Si le Fournisseur propose d'effectuer le transfert des données à caractère personnel sur la base d'une ou de plusieurs de ces dérogations, vous devez consulter votre Équipe juridique.

| Mécanisme de transfert | Explication et mesure |
|---|---|
| Clauses contractuelles types (« CCT ») | • Document de la Commission européenne qui est inséré dans un contrat et qui impose des obligations aux parties afin de veiller à ce que les transferts de données se fassent dans le respect des droits et des libertés des personnes concernées conformément au droit européen.<br>• Les CCT appropriées à utiliser entre Eurotunnel et un Fournisseur seront les CCT régissant le transfert du responsable du traitement vers le sous-traitant conformément à l'Annexe 4.<br>• **Mesure** = Si le Fournisseur propose d'effectuer le transfert des données à caractère personnel sur la base des CCT, suivre la procédure prévue à l'Option A de l'Annexe 3. |

| | |
|---|---|
| Privacy Shield | • Cadre régissant les transferts de données commerciaux effectués entre les organisations européennes et des États-Unis.<br>• L'organisation américaine s'engage à traiter, conserver et transférer ultérieurement les données conformément aux règles européennes en matière de protection des données.<br>• **Mesure** = Si le Fournisseur propose d'effectuer le transfert des données à caractère personnel sur la base du Privacy Shield, suivre la procédure prévue à l'Option B de l'Annexe 3. |
| Règles d'entreprise contraignantes (« REC ») | • Ensemble de règles internes juridiquement contraignantes régissant les transferts de données effectués par une organisation entre l'EEE et les pays non membres de l'EEE.<br>• Le RGPD reconnaît les REC aussi bien pour les responsables du traitement que pour les sous-traitants.<br>• **Mesure** = Si le Fournisseur propose d'effectuer le transfert des données à caractère personnel sur la base des REC, suivre la procédure prévue à l'Option C de l'Annexe 3. |