Annexe Protection des Données Personnelles

La présente annexe a pour objet de définir les conditions dans lesquelles le Prestataire s'engage, en sa qualité de Sous-traitant tel que défini ci-après, à effectuer pour le compte du Client les opérations de traitement de Données à caractère personnel dans le cadre du Contrat.

Le Prestataire est autorisé à traiter pour le compte du Client les Données Personnelles nécessaires pour fournir le Service. La nature des opérations réalisées sur les Données Personnelles est leur stockage et mise à disposition contrôlée auprès des Utilisateurs. Les finalités du Traitement, liste des Données Personnelles traitées et catégories de Personnes Concernées sont définies ci-après.

1. Définitions

Pour les besoins de la présente annexe et nonobstant toute autre définition prévue dans le Contrat, les présents termes commençant par une majuscule, qu'ils soient au singulier ou au pluriel, ont la signification suivante :

Lois et Réglementations sur la Protection des Données à Caractère Personnel : les lois et réglementations en vigueur au sein de l'Union Européenne, de l'Espace Economique Européen et de leurs Etats membres relatives au traitement des Données à caractère personnel, notamment la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dans sa version en vigueur (la « Loi Informatique et Libertés ») et le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (le « Règlement Général sur Protection des Données » ou le « RGPD »). Ainsi que toute réglementation en vigueur au Canada concernant la protection des renseignements personnels (RPRP), incluant sans s'y limiter (i) la loi fédérale « *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, ch. 5) », et (ii) les lois provinciales applicables. Au Québec, la loi provinciale applicable est la « *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) ».

Personne Concernée : toute personne physique identifiée ou identifiable dont les Données à caractère personnel la concernant font l'objet d'un Traitement. Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, un identifiant en ligne.

Responsable du Traitement : toute entité déterminant les finalités et les moyens du Traitement. Pour les besoins du Contrat, le Client agit à l'égard du Prestataire en qualité de Responsable du Traitement.

Sous-traitant : une entité traitant des Données à caractère personnel pour le compte, sur instruction et sous l'autorité du Responsable du Traitement. Lorsqu'il donne accès au Service, le Prestataire agit en qualité de Sous-traitant.

Traitement : toute opération ou tout ensemble d'opérations effectués ou non à l'aide de procédés automatisés et appliqués à des Données à caractère personnel ou des ensembles de Données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, 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, la limitation, l'effacement ou la destruction.

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

2. Objet du Traitement

Le Prestataire est autorisé à traiter pour le compte du Client les Données Personnelles nécessaires pour fournir des Services décrits dans les Conditions Particulières.

Les Données à Caractère Personnel font l'objet des activités de traitement de base suivantes :

Organisation ; Conservation ; Hébergement ; Maintenance ; Consultation, Diffusion, Saisie, Enregistrement et Modification par le Client.

La finalité du Traitement est l'exécution des Services décrits dans les Conditions Particulières.

Les Données à caractère personnel traitées concernent les catégories de données suivantes :

- Données d'identification : prénom, nom de famille, numéro de téléphone adresse courriel, la photographie de profil utilisateur.
- Données professionnelles : fonction, organigramme, etc.
- Données de connexion : logs
- Données Internet : cookies, IP

Les catégories de Personnes Concernées sont les Utilisateurs et personnes physiques autorisées dont l'identification est nécessaire pour assurer la finalité du Service.

Les Données Personnelles sont collectées par le Client qui les saisit ou les importe sur la plateforme hébergeant le service. Il importe également les documents nécessaires au Traitement, documents pouvant inclure des Données Personnelles et renseigne les niveaux d'autorisation à accorder aux Utilisateurs du Services.

3. Obligations Générales

Le Prestataire s'engage à :

- traiter les Données Personnelles uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet des Services décrits dans les Conditions Particulières.
- traiter les Données Personnelles conformément aux instructions documentées du Client. Si le Prestataire considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le Client. En outre, si le Prestataire est tenu de procéder à un transfert de Données Personnelles vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
- garantir la confidentialité des Données Personnelles traitées dans le cadre du présent Contrat
- veiller à ce que les personnes autorisées à traiter les Données Personnelles en vertu du présent Contrat :
    - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
    - reçoivent la formation nécessaire en matière de protection des Données Personnelles
- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des Données Personnelles dès la conception et de protection des Données Personnelles par défaut.

4. Instructions du Client

Le Service est un service standard utilisable à l'identique par tous les clients.

Le Contrat vaut, au jour de signature, instruction écrite du Client au Prestataire de procéder au Traitement dans les termes et limites du Contrat.

5. Sous-Traitance

Le Prestataire est autorisé à faire appel aux sociétés (ci-après, les « sous-traitants ultérieurs ») :

CLARANET	L'hébergement des serveurs sur lesquels sont conservées les Données Personnelles et leur connexion au réseau internet
OVH	L'hébergement des serveurs sur lesquels sont conservées les Données Personnelles et leur connexion au réseau internet

Le Prestataire peut faire appel à un ou plusieurs autres sous-traitants pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Client de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Le responsable de traitement dispose d'un délai de dix (10) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Client n'a pas émis d'objection pendant ce délai.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent Contrat pour le compte et selon les instructions du Client. Il appartient au Prestataire de s'assurer que le sous-traitant ultérieur présente les mêmes 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 RGPD. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des Données, le Prestataire demeure pleinement responsable devant le Client de l'exécution par le sous-traitant ultérieur de ses obligations.

6. Droit d'information des personnes concernées

Il appartient au Client de fournir l'information aux Personnes Concernées (les Utilisateurs du Service) par les opérations de Traitement au moment de la collecte des Données Personnelles.

7. Exercice du droit des personnes

Le Prestataire doit répondre, au nom et pour le compte du Client et dans les délais prévus par la règlementation sur la protection des données aux demandes des Personnes Concernées applicable en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent Contrat.

8. Notification des violations de données à caractère personnel

Le Prestataire notifie au Client toute violation de Données Personnelles dans un délai maximum de quarante-huit (48) heures après en avoir pris connaissance, par courrier électronique au délégué à la protection des données du Client ou au Représentant Autorisé. Cette notification est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La notification contient au moins :

- la description de la nature de la violation de Données Personnelles 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 Personnelles concernés ;
- 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 ;

- la description des conséquences probables de la violation de Données Personnelles ;
- la description des mesures prises ou que le Prestataire propose de prendre pour remédier à la violation de Données Personnelles, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

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

La notification à la Personne Concernée est effectuée par le Client, seul capable d'apprécier le risque pour les droits et libertés d'une personne physique.

9. Aide du Prestataire dans le cadre du respect par le Client de ses obligations

Le Prestataire aide le Client pour la réalisation d'analyses d'impact relative à la protection des Données Personnelles.

Le Prestataire aide le Client pour la réalisation de la consultation préalable de l'autorité de contrôle.

10. Mesures de sécurité

Le Prestataire s'engage à mettre en œuvre les mesures de sécurité prévues par la Charte Qualité et le Contrat.

11. Sort des Données Personnelles

Au terme du Contrat le Prestataire s'engage, à détruire toutes les Données Personnelles. Une fois détruites, le Prestataire doit justifier par écrit de la destruction. Voir Article Réversibilité des CGV

12. Registre des catégories d'activités de traitement

Le Prestataire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client comprenant :

- le nom et les coordonnées du Client pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du Client ;
- dans le cas express d'une injonction judiciaire, les transferts de Données Personnelles 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 du RGPD, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
    - la pseudonymisation et le chiffrement des données à caractère personnel ;
    - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
    - 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 ;
    - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

13. Documentation

Le Prestataire met à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le Client ou

un autre auditeur qu'il a mandaté, et contribuer à ces audits.

14. Délégué à la Protection des Données

Le délégué à la protection des données du Prestataire est : contact-DPO@dilitrust.com