

## ANNEXE SUR LA PROTECTION DES DONNEES

### 1 Définitions

- 1.1 Dans le cadre de la présente Annexe, les termes commençant par une majuscule, utilisés en singulier ou en pluriel, ont la signification qui leur est conférée à son article 12.
- 1.2 Les termes « personne concernée », « traitement », « responsable du traitement » respectivement « maître du fichier » et « sous-traitant » utilisés dans la présente Annexe ont le sens qui leur est conféré par le RGPD respectivement la Législation suisse sur la protection des données, en fonction de leur champ d'application respectif.

### 2 Législations sur la protection des données

Les Parties reconnaissent et conviennent que les législations suivantes relatives à la protection des données peuvent, suivant les circonstances, s'appliquer au traitement des Données Personnelles Client :

- a. le Règlement européen sur la protection des données ;
- b. la Législation suisse sur la protection des données ;

### 3 Traitement des données

#### 3.1 Rôles et conformité

- 3.1.1 Responsabilité du sous-traitant et du responsable du traitement / maître du fichier. Si le Règlement européen sur la protection des données, respectivement la Législation suisse sur la protection des données, s'applique au traitement des Données Personnelles Client, les Parties reconnaissent et conviennent que :
  - a. le Prestataire est un sous-traitant des Données Personnelles Client en vertu du Règlement européen sur la protection des données, respectivement de la Législation suisse sur la protection des données ;
  - b. le Client est un responsable du traitement respectivement maître du fichier ou un sous-traitant d'un tiers, selon le cas, de ces Données Personnelles Client en vertu du Règlement européen sur la protection des données, respectivement de la Législation suisse sur la protection des données ; et
  - c. chaque Partie se conformera aux obligations qui lui sont applicables en vertu du Règlement européen sur la protection des données et/ou de la Législation suisse sur la protection des données en ce qui concerne le traitement des Données Personnelles Client.

3.1.2 Autorisation par un responsable du traitement tiers. Si le Règlement européen sur la protection des données s'applique au traitement des Données Personnelles Client et que le Client est un sous-traitant d'un tiers, le Client garantit au Prestataire que les instructions et actions du Client concernant les Données Personnelles Client, y compris la nomination du Prestataire, pour la réalisation des Services, comme autre sous-traitant, ont été autorisées expressément et préalablement par le responsable du traitement concerné.

3.1.3 Autres législations. Si la Législation d'autres Etats relative à la protection des données s'applique au traitement des Données Personnelles Client, le Client s'engage envers le Prestataire à se conformer aux obligations qui lui sont applicables en ce qui concerne le traitement des Données Personnelles Client et d'informer le Prestataire par écrit de toute disposition contenue dans une telle législation qui pourrait avoir un impact sur le traitement de Données Personnelles Client par le Prestataire en tant que sous-traitant du Client.

### 3.2 **Etendue du traitement**

3.2.1 Nature et finalité du traitement. Le Prestataire traitera les Données Personnelles Client transmises, stockées, ou de toute autre manière traitée par le Client, ou toute personne ou entité agissant pour le Client, via les Services dans le but de fournir les Services et le support technique associé au Client conformément au Contrat et, en particulier, à la présente Annexe.

3.2.2 Instructions du Client. Par la conclusion du Contrat, le Client donne instruction au Prestataire, et s'engage à ne donner instruction au Prestataire, de ne traiter les Données Personnelles Client que dans le strict respect de la législation applicable et au demeurant :

- a. si le Règlement européen sur la protection des données s'applique, uniquement pour fournir les Services et le support technique associé, tel que documenté (i) dans tout Contrat, y compris la présente Annexe, ou (ii) de toute autre manière par écrit ;
- b. si la Législation suisse sur la protection des données s'applique au traitement des Données Personnelles Client, que concernant des traitements que le Client serait en droit d'effectuer lui-même et pour autant qu'aucune obligation légale ou contractuelle de garder le secret n'interdit l'intervention du Prestataire.

3.2.3 Conformité du Prestataire aux instructions. Le Prestataire s'engage à se conformer aux instructions décrites dans la section 3.2.2 sauf si une législation applicable au Prestataire nécessite que des Données Client fassent l'objet d'un traitement spécifique.

### 3.3 **Catégories de données personnelles et de personnes concernées**

Si le RGPD s'applique au traitement Données Personnelles Client par le Prestataire, les informations relatives aux catégories de données personnelles et de personnes concernées doivent figurer dans le contrat en vertu duquel le Prestataire effectue ce traitement.

Le Client s'engage à fournir au Prestataire et à maintenir à jour, une liste des catégories de Données Personnelles Client à laquelle le Prestataire pourra avoir accès durant les Services, ainsi qu'une liste des catégories de personnes concernées en contactant le Prestataire à l'adresse mentionnée comme "Contact du Prestataire en matière de protection des données" (article 10 ci-dessous). Ces listes font partie intégrante du Contrat.

Si le Client ne précise pas les informations requises, le Prestataire partira du principe qu'il pourra avoir accès, durant les Services, à tous les types de données fournis par le Client, ce qui peut inclure toutes les catégories de Données Personnelles Client, et à traiter les Données Personnelles Client relatives à toutes les catégories de personnes concernées.

Le Prestataire décline toute responsabilité en lien avec l'omission du Client de préciser ces informations en temps utile.

## 4 Suppression de données

- 4.1 **Suppression pendant la Durée de validité.** Le Prestataire permet au Client de supprimer ou modifier des Données Personnelles Client pendant la durée du Contrat pour autant que cette suppression soit compatible avec la fonctionnalité des Services.
- 4.2 **Suppression à la fin du Contrat.** Le Client requiert irrévocablement au Prestataire de supprimer à la fin du Contrat, toutes les Données Client (y compris toutes copies existantes) des systèmes du Prestataire, conformément au droit applicable. Le Prestataire se conformera à cette instruction dans les plus brefs délais, sauf si le Prestataire doit conserver tout ou partie des Données Client pour un motif technique ou légal. Le Client reconnaît et accepte qu'il est de son unique responsabilité de transférer et/ou sauvegarder les Données Client qu'il souhaite conserver par la suite.

## 5 Sécurité des données

### 5.1 Mesures de sécurité

- 5.1.1 Mesures de sécurité du Prestataire. Le Prestataire met en œuvre et maintient des mesures techniques et organisationnelles appropriées pour protéger les Données Client contre un incident de sécurité. Ces mesures comprennent notamment :

- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- les moyens pour limiter l'accès aux Données Client au personnel ayant un besoin d'y accéder dans le cadre de la fourniture des Services ;
- les moyens permettant de rétablir la disponibilité des Données Personnelles Client et l'accès à celles-ci dans des délais appropriés en cas d'Incident de sécurité ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

- 5.1.2 Conformité de sécurité par le personnel du Prestataire. Le Prestataire prendra des mesures appropriées pour assurer le respect des mesures de sécurité susvisées par ses employés et sous-traitants, notamment en veillant à ce que toutes les personnes autorisées à traiter les Données Personnelles Client s'engagent à respecter la confidentialité ou soient soumises à une obligation légale de confidentialité appropriée.

### 5.2 Incidents de sécurité

- 5.2.1 Notification au Client d'Incident de sécurité. Si le Prestataire prend connaissance d'un Incident de sécurité, le Prestataire s'engage à en informer dans les meilleurs délais le Client par tout moyen utile (notamment via la personne de contact indiquée par le Client). Le Prestataire décrira, dans la mesure du possible, la nature de l'Incident de sécurité, ainsi que les mesures éventuellement prises par le Prestataire pour atténuer les risques potentiels et les mesures que le Prestataire recommande au Client de prendre. Les agissements du Prestataire en lien avec cet article 5.2.1 ne constitueront pas, et ne pourront pas être interprétés comme une reconnaissance par le Prestataire de toute faute ou responsabilité en lien avec l'Incident de sécurité intervenu.

5.2.2 **Obligations du Client.** Le Prestataire n'évaluera pas le contenu des Données Client afin d'identifier le type de données concernées. Le Client est seul responsable d'effectuer toute analyse de ces Données Client et de se conformer aux dispositions légales qui lui sont applicable, notamment à son éventuelle obligation de notifier l'Incident de sécurité à toute autorité compétente et/ou aux personnes concernées. Dans ce cadre, le Prestataire fournira au Client toute assistance raisonnablement requise par celui-ci afin de se conformer à ses obligations.

### 5.3 Renseignements et audits sur les mesures de sécurité

5.3.1 **Renseignements.** Si le Règlement européen sur la protection des données s'applique au traitement de Données Personnelles Client, le Prestataire met à la disposition du Client, en plus des informations contenues dans le Contrat, y compris la présente Annexe, tous les documents et informations raisonnablement nécessaires afin de démontrer la conformité du Prestataire au RGPD et à ses obligations en découlant.

5.3.2 **Droit d'audit.** Le Prestataire autorisera le Client ou un auditeur indépendant désigné par le Client à effectuer des audits (y compris des inspections) afin de vérifier le respect des obligations du Prestataire avec ses obligations découlant du RGPD. Le Prestataire contribuera de manière raisonnable aux audits décrits dans cet article 5.3.2. Dès la conclusion de l'audit, le Client transmettra le rapport d'audit complet au Prestataire, sans frais.

5.3.3 **Requête.** Toute demande en vertu des articles 5.3.1 ou 5.3.2 ci-dessus doit être communiquée au Prestataire par écrit et indiquer (i) les Données Personnelles Client concernées, (ii) les motifs pour lesquels les conditions visées aux articles 5.3.1 ou 5.3.2 ci-dessus sont réalisées pour ces données, (iii) les documents spécifiques dont la prise de connaissance est requise, respectivement les obligations spécifiques du Prestataire sur lesquelles l'audit doit porter et (iv) que le Client s'engage expressément à n'utiliser les informations recueillies que pour s'assurer du respect par le Prestataire de ses obligations par rapport aux Données Personnelles Client et notamment que les informations recueillies ne seront pas utilisées dans le cadre d'une procédure judiciaire ou administrative à l'encontre du Prestataire. Sauf circonstances exceptionnelles, le Client ne peut pas effectuer plus d'une requête par année.

5.3.4 **Exercice.** Après réception par le Prestataire d'une requête conforme à l'article 5.3.3 ci-dessus, et pour autant que toutes les conditions soient réalisées, le Prestataire donnera suite à la requête comme suit :

- a. Le Prestataire indiquera au Client, s'agissant de la consultation de documents (article 5.3.1 ci-dessus), la période durant laquelle il peut consulter les documents au siège du Prestataire. Sauf accord express contraire du Prestataire, le Client n'est pas autorisé à effectuer des copies des documents consultés. Alternativement, le Prestataire peut décider de communiquer les documents par tout autre moyen utile, notamment en les adressant par voie électronique ;
- b. Le Prestataire informera le Client, s'agissant des audits (article 5.3.2 ci-dessus) (i) la ou les dates auxquelles les audits pourront avoir lieu et (ii) l'étendue de l'audit, notamment les inspections qui pourront être effectuées, afin de contrôler le respect par le Prestataire de ses obligations en vertu de la présente Annexe. Les coûts internes du Client respectivement les frais de l'auditeur indépendant désigné par celui-ci sont entièrement à la charge du Client. Le Prestataire peut refacturer au Client ses propres frais pour la mise en place et l'exécution de l'audit, basés sur les coûts engendrés par le Prestataire. Le Prestataire peut s'opposer à tout auditeur indépendant nommé par le Client si, de l'avis du Prestataire, l'auditeur n'est pas suffisamment qualifié, est un concurrent du Prestataire, ou de toute autre manière ne serait pas en mesure de

réaliser sa mission convenablement. Dans ce cas, le Client pourra soit effectuer l'audit lui-même, soit proposer au Prestataire un autre auditeur.

- 5.3.5 **Informations confidentielles.** Les dispositions contenues au présent article 5.3 ne sauraient être interprétées comme imposant au Prestataire de communiquer au Client (i) toute information relative à des secrets d'affaires le concernant, respectivement toute information à caractère confidentiel, ou (ii) toute information concernant des clients du Prestataire (hormis le Client). Le Prestataire peut subordonner la consultation de documents (article 5.3.1 ci-dessus) ou la conduite d'audit (article 5.3.2 ci-dessus) à la signature d'une convention de confidentialité spécifique.

## 6 Assistance du Prestataire

- 6.1 **Conformité.** Le Prestataire fournira au Client toutes les informations nécessaires afin que le Client puisse apporter la preuve du respect de ses obligations aux termes du Règlement européen sur la protection des données, respectivement de la Législation suisse sur la protection des données. Le Client s'engage également à fournir au Prestataire toutes les informations nécessaires afin de permettre au Prestataire d'apporter la preuve du respect de ses obligations aux termes du Règlement européen sur la protection des données, respectivement de la Législation suisse sur la protection des données.
- 6.2 **Demandes de personnes concernées.** Si le Prestataire reçoit une demande d'une personne concernée concernant des Données Personnelles Client, le Prestataire transférera la demande dès réception au Client. Le Prestataire informera du transfert la personne concernée en précisant les coordonnées du Client, la date de transfert et en précisant que le Client sera désormais seul responsable de répondre à sa demande. Les Parties conviennent qu'il est de la responsabilité exclusive du Client de donner suite ou non aux demandes de personnes concernées.
- 6.3 **Actions par le Client.** Le Prestataire assistera le Client à se conformer à ses obligations légales vis-à-vis des personnes concernées, dans la mesure raisonnablement exigible et pour autant que cela soit compatible avec les fonctionnalités des Services. Les mesures porteront sur tous les droits conférés à la personne concernée par la législation sur la protection des données qui lui est applicable, notamment l'accès, la rectification, la limitation, l'opposition, la suppression et la portabilité des Données Personnelles Client la concernant.
- 6.4 **Analyses d'impact et consultation préalable.** Si le Règlement européen sur la protection des données s'applique au traitement de Données Personnelles Client, le Prestataire s'engage, dans la mesure où cela peut raisonnablement être exigé de lui, compte tenu de la nature du traitement et des informations à sa disposition, à assister le Client, à assurer le respect de ses obligations en matière d'analyse d'impact et de consultation préalable conformément aux articles 35 et 36 RGPD.

## 7 Transferts de données

- 7.1 **Pays autorisés.** Sauf stipulation contraire dans le Contrat, le Client accepte que le Prestataire stocke et traite les Données Client en Suisse, en France et au Canada et dans tout autre pays membre de l'Union Européenne ou assurant un niveau adéquat de protection des données personnelles dans lequel Le Prestataire ou l'un de ses sous-traitants maintient des installations.

- 7.2 **Autorisation spéciale.** Le Prestataire informera (sauf si le Prestataire est tenu par une obligation légale de ne pas divulguer) le Client préalablement à tout transfert de Données Personnelles Client vers un état non mentionné à l'article 7.1 ci-dessus et le Client s'engage à autoriser ledit transfert pour autant que le Prestataire puisse garantir par tout moyen utile un niveau de protection adéquat des Données Personnelles Client.

## 8 Sous-délégation

- 8.1 **Consentement.** Le Client autorise spécifiquement le Prestataire à faire appel à d'autres sous-traitants, lesquels peuvent être des Entités Affiliées du Prestataire ou d'autres tiers. Si le Règlement européen sur la protection des données s'applique, le Prestataire s'engage à informer préalablement et par écrit le Client de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants pour lui permettre de formuler des objections à l'encontre desdits sous-traitants.
- 8.2 **Exigences.** Le Prestataire s'engage, en cas de délégation conformément à l'article 8.1 ci-dessus à s'assurer par écrit que :
- le sous-traitant n'accède et ne traite des Données Client que dans la mesure requise pour exécuter les obligations qui lui sont confiées ; et
  - si le Règlement européen sur la protection des données s'applique, les obligations énoncées à l'article 28 (3) du RGPD sont imposées au sous-traitant.
- 8.3 **Objection.** Si le Règlement européen sur la protection des données s'applique, le Client dispose d'un délai de 30 jours après avoir été informé de l'ajout ou du remplacement prévu d'un sous-traitant (y compris le nom et l'emplacement du sous-traitant concerné et les activités qu'il effectuera) pour présenter ses objections. Si le Prestataire confirme au Client la nomination du sous-traitant, le Client est en droit de résilier le Contrat applicable avec effet immédiat par notification écrite adressée dans un délai de 14 jours dès réception de la confirmation du Prestataire. Ce droit de résiliation est le seul et unique recours du Client en cas d'objection à un nouveau sous-traitant. La non-réaction du Client à l'un ou l'autre des délais visés à cet article 8.3 sera interprétée comme une acceptation du nouveau sous-traitant.

## 9 Registre des traitements

Le Client reconnaît que le Prestataire peut être tenu, notamment par le Règlement européen sur la protection des données de : (a) collecter et conserver certaines informations, y compris le nom et les coordonnées de chaque sous-traitant et/ou responsable du traitement avec lesquels le Prestataire agit et, le cas échéant, le représentant local du responsable du traitement et/ou le délégué à la protection des données ; et b) remettre ces informations à la disposition de toute autorité compétente. Le Client s'engage à fournir au Prestataire toutes informations raisonnablement nécessaires au Prestataire pour exécuter ses obligations.

## 10 Contact du Prestataire en matière de protection des données

L'interlocuteur chez le Prestataire en matière de protection des données peut être contacté à l'adresse suivante : [privacy@groupe-t2i.com](mailto:privacy@groupe-t2i.com).

## 11 Contact du Client en matière de protection des données

11.1 **Délégué à la protection des données.** Si le RGPD impose au Client de nommer un délégué à la protection des données, le Client doit en communiquer les coordonnées au Prestataire. Le Prestataire est tenu de conserver les coordonnées du délégué à la protection des données du Client dans un registre des traitements. En ne communiquant pas au Prestataire les coordonnées d'un délégué à la protection des données, le Client confirme au Prestataire qu'il n'est pas tenu d'en nommer un.

11.2 **Personne de contact.** Si le RGPD n'impose pas au Client de nommer un délégué à la protection des données, le Client peut néanmoins indiquer au Prestataire les coordonnées de sa personne en charge des questions relatives à la protection des données. Cette personne sera le point de contact privilégié du Prestataire pour toutes les communications relatives à la protection des données, favorisant ainsi un transfert de l'information plus rapide et efficace.

## 12 Définitions

|  |   |
|--|---|
| <b>Annexe</b>  | désigne la présente annexe.   |
| <b>Contrat</b>   | désigne le contrat dans lequel la présente Annexe est intégrée, tel que modifié par voie d'avenant, le cas échéant, entre le Client et le Prestataire ayant pour objet la réalisation de Services.  |
| <b>Données Client</b>  | désigne les données (i) transmises par le Client au Prestataire, ou récoltées par le Prestataire auprès du Client, dans le cadre de l'exécution des Services (ii) et qui sont détenues ou traitées par le Prestataire.  |
| <b>Données Personnelles Client</b>                                     | désigne les données à caractère personnel ou données personnelles, c'est-à-dire toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, selon et conformément à la législation sur la protection des données applicable à ces données, contenues dans les Données Client. |
| <b>Entité Affiliée</b>   | désigne toute entité contrôlant, contrôlée par, ou sous un contrôle commun avec, une Partie. Pour les besoins de cette définition « contrôler » désigne : (a) la titularité d'au moins 50% du capital de l'entité ; (b) la titularité d'au moins 50% des droits de vote au sein de l'entité ; ou (c) le pouvoir d'exercer une influence déterminante sur la direction de l'entité.  |
| <b>Incident de sécurité</b>  | désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Client ou l'accès non autorisé à des Données Client.  |
| <b>Législation d'autres Etats relative à la protection des données</b> | toute législation relative à la protection des données autre que la Législation suisse sur la protection des données et le Règlement européen sur la protection des données.  |
| <b>Législation suisse sur la protection des données</b>                | désigne la loi fédérale sur la protection des données du 19 juin 1992 (Suisse) et ses ordonnances d'application, ainsi que les différentes lois cantonales sur la protection des données et leur ordonnance d'application. En Suisse, dans le cas des administrations publiques cantonales et communales, la législation cantonale sur la protection des données s'applique en priorité.  |
| <b>Règlement européen sur la protection des données (RGPD)</b>         | désigne 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 ( <b>RGPD</b> ).   |
| <b>Services</b>  | désigne tous les Services fournis par le Prestataire au Client sous le Contrat.   |