

ANNEXE B – Accord de traitement de données (DPA)

Dans le cadre de l'exécution du Contrat, MISSION RGPD a accès aux données à caractère personnel traitées sous la responsabilité du Client lequel agit en qualité de responsable de traitement.

En conséquence, la réglementation en matière de protection des données personnelles (ci-après la « Réglementation ») s'applique à la relation contractuelle précitée.

C'est dans ce contexte qu'a été adoptée la présente annexe, ci-après dénommée « l'Accord », partie intégrante du Contrat conclu entre les Parties afin de s'assurer que les Parties sont en conformité avec la Réglementation et notamment à l'article 28 du RGPD.

1. Caractéristiques du traitement

Par « traitement de données » sont comprises les opérations de collecte, d'enregistrement, d'organisation, de conservation, d'extraction et de consultation des Données personnelles.

Le traitement des Données a pour objet, nature et finalité la mise à disposition d'un logiciel de gestion de l'activité en matière de protection des données personnelles au sein de l'organisation du Client. Les traitements de données qui découlent de l'utilisation de l'application sont les suivants : gestion des comptes utilisateurs de la plateforme et le suivi des demandes de droits. Le logiciel étant disponible en saas uniquement, l'hébergement des données est également assuré par Mission RGPD.

Les Données sont conservées pendant toute la durée de la relation commerciale entre le Client et MISSION RGPD.

Les personnes concernées par le traitement sont :

- Les utilisateurs de la plateforme DATA COMPLY ONE ;
- Les personnes identifiées dans les documents téléchargés par le Client ou mentionnées dans les différents modules du Service Applicatif, dont les personnes exerçant leurs droits auprès du Client.

Les Données relèvent des catégories de données suivantes :

- Les données relatives à l'identification, dont notamment les données d'état civil (nom, prénom, adresse mail personnelle dans le cas de certaines demandes de droits) ;
- Les données professionnelles (adresse mail professionnelle, entité de rattachement) ;
- Toutes Données importées de manière autonome sur la plateforme par le Client et les utilisateurs du Service ;
- Les données de connexion (notamment identifiant, journaux de connexion).

2. Obligations du Client

Dans le cadre des présentes, le Client a défini seul les finalités et les moyens de traitement. En conséquence et conformément à la Réglementation, le Client revêt la qualité de responsable de traitement.

Dès lors, le Client s'engage à faire sienne l'ensemble des obligations qui s'imposent à tout responsable de traitement.

2.1 Les garanties

Le Responsable du traitement garantit que les activités de traitement confiées au Sous-traitant, et

notamment les Données personnelles dont il lui confie le traitement, respectent les principes de la Réglementation et notamment :

- Le caractère loyale, licite, transparent de la collecte ;
- La légitimité de la ou des bases légales choisies ;
- Le caractère déterminé, explicite et légitime des finalités poursuivies ;
- La minimisation des données collectées ainsi que leur adéquation, leur pertinence au but poursuivi ;
- L'exactitude et la mise à jour des Données personnelles en cause ;
- La limitation, la détermination des durées de conservation et les modalités du cycle de vie des Données personnelles ;
- La sécurité appropriée mise en œuvre pour les Données personnelles en amont ou en aval des activités de traitement confiées au Sous-traitant ;
- Les enjeux d'accountability, de privacy by design et de privacy by default ;
- La réalisation de toutes les procédures et formalités requises par le traitement ;
- L'information exhaustive des Personnes concernées conformément à la Réglementation notamment concernant les droits et les transferts opérés auprès du Sous-traitant ou à d'autres destinataires.

2.2 Les instructions

Le Responsable du traitement s'engage à respecter la Réglementation. Il doit avoir exprimé ses besoins en matière de protection des Données personnelles de manière précise, à l'écrit, au regard des risques que présente le traitement. Ces instructions doivent être formalisées à l'écrit sur un support à même d'être conservé. Le Responsable du traitement aura la charge de cette conservation et devra s'assurer de la conformité de ces instructions à la Réglementation.

Toute évolution dans le cadre de ces instructions devra être notifiée au plus vite au Sous-traitant. Il en va de même pour un changement de périmètre de traitement confié que ce soit au regard des finalités poursuivies ou des modalités de traitement.

Tout demande de changement de périmètre fera l'objet d'une étude de faisabilité par le Sous-traitant et la formalisation d'un devis.

Il incombe au Responsable du traitement d'assurer le suivi, le pilotage et la supervision des activités de traitement confiées au Sous-traitant.

2.3 Les mesures techniques et organisationnelles du Sous-traitant

Le Responsable du traitement déclare expressément avoir pris connaissance des mesures techniques et organisationnelles et plus largement les ressources mises en œuvre par le Sous-traitant dans le cadre du présent accord lesquelles constituent des garanties suffisantes de la conformité du Sous-traitant et de ses prestations à la Réglementation notamment mais non exclusivement au regard de la sécurité, de la confidentialité, de l'exercice du droit des personnes concernées, de l'assistance et la coopération du Sous-traitant.

La mise en œuvre de mesures supplémentaires pourra être négociée d'un commun accord entre les Parties en contrepartie du paiement des prestations supplémentaires.

3. Les obligations de MISSION RGPD

3.1 Instructions du Responsable de traitement

Le Sous-traitant traite les données personnelles pour le compte du Responsable du traitement dans la limite du périmètre de traitement décrit au sein du Contrat et conformément aux instructions documentées du Responsable du traitement.

Le Sous-traitant n'est en aucun cas tenu de suivre des instructions non documentées par écrit ou contraires à la Réglementation et il ne saurait voir sa responsabilité engagée à ce titre.

Si le Sous-traitant estime qu'une instruction du Responsable du traitement constitue une violation de la Réglementation, il l'informe dans les meilleurs délais étant entendu qu'une telle obligation ne saurait s'apparenter à une obligation générale de conseil ou à une obligation de veille juridique ou encore à une obligation de surveillance ou de vérification de la conformité du Responsable du traitement de manière générale ou spécifique.

3.2 Transferts de données hors Union européenne

MISSION RGPD s'efforce de conserver les Données personnelles au sein de l'Union Européenne. A ce titre MISSION RGPD exige que les Données transférées à ses sous-traitants soient hébergées sur le territoire de l'Union européenne. La mise à disposition de la plateforme n'entraîne aucun transfert hors UE.

En tout état de cause, MISSION RGPD assure de faire tous les efforts pour mettre en œuvre les garanties nécessaires et suffisantes afin d'assurer le niveau de protection requis par la Réglementation. Soucieux de la sécurité et de la confidentialité des Données, MISSION RGPD s'engage, si des Données personnelles sont transférées hors UE, à ce que tous les transferts s'effectuent à destination :

- Soit d'un pays reconnu par la Commission européenne comme assurant un niveau de protection adéquat ;
- Soit vers un pays n'offrant pas de protection adéquate mais dont le transfert est permis en application de la Réglementation applicable notamment en étant encadré par les clauses contractuelles types de la Commission européenne dont la CNIL a préalablement reconnu qu'elles permettent de garantir un niveau de protection suffisant de la vie privée et des droits fondamentaux des personnes.

3.3 Registre de sous-traitance

Le Sous-traitant tient un registre de sous-traitance conformément à l'article 30 du RGPD. Ce registre recense l'ensemble des traitements réalisés pour le compte du Responsable du traitement sans que cela n'exonère ce dernier de tenir son propre registre.

3.4 Confidentialité

Le Sous-traitant fera ses meilleurs efforts pour s'assurer que les personnes autorisées à intervenir dans le traitement de données soient soumises à un engagement de confidentialité ou à une obligation légale appropriée de confidentialité.

3.5 Sécurité

MISSION RGPD a l'obligation d'assurer la sécurité des Données afin notamment d'empêcher toute perte, endommagement, altération ou accès non-autorisé aux Données. A ce titre, MISSION RGPD s'engage à mettre en place toutes les mesures techniques, organisationnelles et matérielles nécessaires en tenant compte de la nature des

Données en vue et pendant toute la durée de leur traitement par ses soins.

Le Responsable du traitement apprécie l'adéquation des mesures de sécurité aux enjeux et aux risques inhérents au Traitement. Il donne son accord pour sa mise en œuvre dans les conditions de sécurité décrites par le Sous-traitant.

Si tel n'est pas le cas et que le Responsable du traitement estime que les mesures en œuvre sont insuffisantes, les Parties s'entendent pour mettre en œuvre, aux frais du Responsable du traitement des mesures additionnelles, le cas échéant figurant en annexe des présentes.

Dans l'hypothèse où, au cours de l'exécution du contrat, le Responsable du traitement était amené à considérer les mesures prises comme insuffisantes, les Parties conviennent expressément de se réunir pour convenir d'un commun accord de nouvelles mesures et leurs modalités de mises en œuvre.

3.6 Sous-traitance ultérieure

Le Sous-traitant est expressément autorisé par le Responsable du traitement à déléguer tout ou partie du traitement qui fait l'objet du présent accord à un sous-traitant ultérieur pour réaliser les activités de traitement sous-traitées au titre du contrat. Le sous-traitant communique au Responsable du traitement sur demande de ce dernier, la liste des sous-traitants ultérieurs qui interviennent dans le traitement de données. Dans le cas où le Sous-traitant fait appel à un nouveau sous-traitant ultérieur ou le remplace, il déclare cette modification au Responsable du traitement dans les meilleurs délais.

Le Sous-traitant s'assure qu'il recrute un sous-traitant ultérieur qui répond aux mêmes exigences en matière de protection des données que celles qui régissent le Contrat avec le Responsable du traitement, afin d'assurer qu'il présente des garanties suffisantes pour assurer la protection des données personnelles.

Le Sous-traitant encadre sa relation avec le sous-traitant ultérieur au moyen d'un contrat conforme à la Réglementation et qui répond notamment aux exigences de l'article 28 du RGPD.

Le Sous-traitant est responsable de la bonne exécution des obligations du sous-traitant ultérieur.

Les catégories de sous-traitants ultérieurs susceptibles d'intervenir sont les suivants :

- Hébergeur,
- Prestataires externes pour l'aide à la mise en conformité,
- Éditeur de solutions logicielles tierces (notamment les options Sauvegarde externalisée, Protection Web et Data Comply One Academy).

3.7 Information et droits des personnes

Le Client reconnaît et accepte les conditions de ce traitement et s'engage à informer les Utilisateurs, au nom et pour le compte de MISSION RGPD, de l'ensemble des caractéristiques du traitement et des modalités d'exercice des droits dont elles disposent. Les utilisateurs ont accès à une Politique de confidentialité dédiée accessible directement depuis la Plateforme. Ils sont informés de leurs droits et des modalités d'exercice dans ce document.

Le Sous-traitant notifiera au Responsable du traitement toute demande d'exercice de droit dont il serait directement destinataire pour le compte du Responsable du traitement afin que ce dernier puisse les traiter. Le Responsable du traitement fera son affaire du traitement des demandes qui lui seront directement adressées.

Le Sous-traitant apportera son concours au Responsable du traitement dans la mesure du possible et dans la limite des informations dont il dispose, pour permettre à ce dernier de répondre à ses demandes d'exercice de droits.

Les prestations réalisées au titre du présent article pourront faire l'objet d'une facturation supplémentaire par le Sous-traitant au Responsable du traitement soumise à devis préalable.

3.8 Notification des incidents de sécurité et violations de données personnelles

Le Sous-traitant doit informer le Responsable du traitement des violations de Données personnelles (au sens du RGPD) dont il a connaissance afin de lui permettre de notifier le cas échéant l'autorité de contrôle voire les personnes concernées. A la demande du Responsable du traitement, le Sous-traitant fera ses meilleurs efforts pour transmettre dans les meilleurs délais au Responsable les informations dont il dispose pour l'aider. Il pourra transmettre ces informations au fur et à mesure qu'il en a connaissance sans que cela ne puisse lui être opposé.

Ces prestations pourront faire l'objet d'une facturation supplémentaire soumise à devis préalable.

4. Collaboration entre les Parties

Le Sous-traitant met à disposition du Responsable du traitement toute la documentation nécessaire pour démontrer le respect de ses obligations au regard de la Réglementation. Il autorise le Responsable du traitement, lorsque celui-ci l'estime nécessaire, à réaliser des audits de conformité du Sous-traitant.