

ANNEXE 1 RGPD DEDALUS HEALTHCARE FRANCE

TOUTES PRESTATIONS DEDALUS HEALTHCARE FRANCE

Article 1 : Dispositions générales

Dans le cadre de la réalisation des Prestations objet du Contrat, le Prestataire est amené à traiter des données à caractère personnel du Client, pour le compte de ce dernier.

En application des présentes, les données du Client comportent des données à caractère personnel, lesquelles font l'objet d'un Traitement, décrit à l'Annexe 1. Chaque Partie s'engage ainsi à se conformer à ses obligations en application de la législation en vigueur relative à la protection des Données à Caractère Personnel, y compris celles de la loi française n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et, à compter du 25 mai 2018, du Règlement général relatif à la protection des données 2016/679 (ci-après RGPD), ci-après Réglementation.

Les Parties s'interdisent de commettre tout acte de nature à mettre l'autre Partie en position de violation desdites législations protectrices des Données à caractère personnel.

Les Parties reconnaissent que la présente Annexe, fait partie intégrante du Contrat. Cette Annexe constitue l'intégralité de l'accord entre les Parties relativement à l'objet de la présente Annexe. En cas de conflit ou d'incohérences entre les stipulations du Contrat et de la présente Annexe, les stipulations de l'Annexe prévaudront.

Article 2 : Obligations du Client

Le Client, en tant que Responsable de traitement, détermine les finalités et les moyens du Traitement envisagé et garantit le Prestataire que le Traitement en cause satisfait aux exigences de la réglementation, notamment que les Données à caractère personnelles sont traitées de manière licite, loyale et transparente, qu'elles ont été collectées pour des finalités déterminées, explicites et légitimes et que l'information requise aux personnes concernées par le Traitement a bien été fournie au moment de la collecte desdites données.

Le Responsable du traitement sera ainsi notamment seul responsable d'informer les personnes concernées quant au traitement de leurs données à caractère personnel et d'obtenir leur consentement lorsque celui-ci s'avère requis, conformément à la Réglementation Applicable

Les Parties reconnaissent et acceptent expressément que le Responsable du traitement et le Sous-traitant engagent leur responsabilité à l'égard des personnes concernées conformément à l'article 82 du RGPD.

A ce titre, le Sous-traitant n'est tenu pour responsable d'un dommage causé par le Traitement que dans la mesure où : (i) il n'a pas respecté les obligations prévues par la présente Annexe et/ou la Réglementation Applicable qui lui incombent spécifiquement ; ou (ii) il a agi en-dehors des instructions licites du Responsable du traitement.

Le Sous-traitant sera exonéré de toute responsabilité lorsque le fait qui a provoqué un quelconque dommage ne lui est pas directement imputable.

Le Client s'engage à documenter, par écrit, toute instruction concernant le Traitement des Données à caractère personnel par le Prestataire. Toute autre instruction, non expressément visée dans la présente annexe, sera documentée par écrit par le Client et adressée au Prestataire, qui s'engage à la respecter selon un échéancier validé par les deux parties. Les contacts des Parties sont listés dans les tableaux des contacts ci-dessous.

Article 3 : Obligations du Prestataire

Il est expressément convenu que le Prestataire :

- Traite les Données à caractère personnel uniquement pour la/les finalité(s) qui font l'objet de la sous-traitance ;
- Ne peut traiter les Données à caractère personnel que sur instructions documentées du Client, y compris en ce qui concerne la localisation de l'hébergement et les transferts vers les pays tiers ;
- Informe le Client avant le début du Traitement si le Prestataire est tenu de procéder à un transfert de Données à caractère personnel vers un pays tiers ou une organisation internationale, en vertu du droit de l'Union Européenne ou du droit de l'Etat membre auquel il est soumis et met en place une garantie appropriée ; cette obligation ne s'applique pas si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- Informe immédiatement le Client si le Prestataire considère qu'une instruction donnée par le Client constitue une violation de la réglementation en matière de protection des Données à caractère personnel ; le Prestataire n'est pas tenu de répondre favorablement à cette instruction dans la mesure où elle représentera une violation du RGPD.
- Garantit la sécurité et la confidentialité des Données à caractère personnel traitées dans le cadre des Prestations ;
- Veille, à cet égard, à ce que les fonctions autorisées à traiter les Données à caractère personnel (cf. Annexe) s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- Prend en compte, s'agissant des prestations qu'il réalise pour le compte du Client, les principes de protection des données dès la conception et par défaut ;
- Peut sous-traiter tout ou partie des activités de traitement réalisées pour le compte du Client, sous réserve d'en avoir informé préalablement le Client, et en l'absence d'opposition de ce dernier dans les 15 jours après avoir reçu cette information ;
- Doit s'assurer que son propre Sous-traitant respecte les obligations des Prestations et que ce Sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences de la Règlementation sur la protection des données à caractère personnel ;
- Aide le Client, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible à s'acquitter de son obligation de donner suite aux demandes des personnes concernées relatives à leurs droits (droits d'accès, de rectification, d'effacement et d'opposition, à la limitation du traitement, à la portabilité, de ne pas faire l'objet d'une décision individuelle automatisée) ; à ce titre, en cas de réception directement par le Prestataire d'une telle demande, il est convenu que celui-ci

transmette la demande au Client, à qui revient la charge d'y apporter une réponse dans les délais prévus par la Règlementation ;

- Aide le Client s'agissant de la réalisation d'analyses d'impact relative à la protection des données, de la communication et de la notification de violations de données, de la réalisation de la consultation préalable de l'autorité de contrôle et de la mise en œuvre de ses propres mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque ;
- Selon le choix du Client, détruit toutes les Données à caractère personnel ou les renvoie au Client au terme de la prestation ou à son nouveau Sous-traitant, étant précisé que le renvoi desdites données doit être accompagné de la destruction par le Prestataire de toutes les copies existantes dans les systèmes d'information de ce dernier. A la réception de toute demande de destruction, le Prestataire procédera à cette destruction, sauf si le droit national du Prestataire en dispose autrement ;
- Met à la disposition du Client toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le Client ou un auditeur choisi par ce dernier, et contribue à ces audits dans les conditions visées ci-dessous.
- Notifie au Client toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance conformément à l'article 33 paragraphe 2 du RGPD.
- Enfin, respecte de manière générale les règles définies dans les articles 28 et 30 du RGPD.

Article 4 : Audit

Le Client, au cours de l'exécution des Prestations, dans la limite d'une (1) fois par année contractuelle, a la possibilité de procéder à ses frais et sous sa responsabilité à un audit ayant pour objet de vérifier la conformité des prestations de sous-traitance effectuées par le Prestataire pour le compte du Client.

Cet audit est notifié par le Client au Prestataire par lettre recommandée avec accusé de réception détaillant les documents demandés et, le cas échéant, le protocole qui sera déroulé, les méthodes utilisées et données auditées, trente (30) jours ouvrés avant la date projetée de sa mise en œuvre.

Il est expressément convenu entre les Parties qu'est privilégiée, dans la mesure du possible, la réalisation d'un audit sur pièces dans le respect de la Politique Qualité interne et qu'un audit sur place serait programmé si les éléments mis à la disposition par le Prestataire ne s'avéraient pas suffisant pour démontrer le respect de ses obligations au titre de la présente clause.

L'audit est effectué par le Client ou par un tiers désigné par lui, à la triple condition que ce tiers ne soit pas un concurrent direct ou indirect du Prestataire, qu'il soit soumis au secret professionnel et qu'il ait conclu un accord de confidentialité.

Il est, par ailleurs, entendu que cette démarche d'audit exclut toute communication de documents de nature financière, comptable ou tenant aux relations du Prestataire avec d'autres clients.

Les résultats d'audit feront l'objet d'un débat contradictoire et d'une validation par les Parties. Les frais d'audit demeureront à la charge du Client, ainsi que les éventuels frais engagés et temps passé par le Prestataire.