Annexe Contractuelle - Données à Caractère Personnel (DPA)

# Article 1 : Définitions

1. **Données à caractère personnel** : Toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée »), telle que définie par le Règlement Général sur la Protection des Données (RGPD).
2. **Responsable de traitement** : La personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement des données à caractère personnel.
3. **Sous-traitant** : La personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du Responsable de traitement.
4. **Traitement** : Toute opération ou ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel.
5. **Violation de données** : Une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l’altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou autrement traitées, ou l’accès non autorisé à de telles données.
6. **Transfert de données** : Tout transfert de données à caractère personnel en dehors de l’Espace Économique Européen (EEE), y compris vers un pays tiers ou une organisation internationale.
7. **Service Cloud** : Tout service de traitement, stockage, ou gestion de données à caractère personnel fourni par le Sous-traitant via des infrastructures cloud.

# Article 2 : Objet

La présente annexe a pour objet de définir les conditions et modalités de traitement des données à caractère personnel dans le cadre du contrat principal, incluant l’utilisation de services cloud. Elle vise à garantir la conformité des parties aux obligations découlant du RGPD et des lois françaises relatives à la protection des données personnelles.

# Article 3 : Obligations du Responsable de traitement

1. **Licéité du traitement** : Le Responsable de traitement s’engage à traiter les données à caractère personnel de manière licite, loyale et transparente conformément aux articles 5 et 6 du RGPD.
2. **Finalités déterminées** : Les données à caractère personnel ne doivent être collectées que pour des finalités déterminées, explicites et légitimes, et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités.
3. **Minimisation des données** : Le Responsable de traitement doit veiller à ce que les données collectées soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
4. **Exactitude des données** : Il incombe au Responsable de traitement de s’assurer que les données à caractère personnel sont exactes et, si nécessaire, tenues à jour.
5. **Sécurité des données** : Le Responsable de traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l’article 32 du RGPD. Cela inclut l’évaluation régulière des mesures de sécurité des services cloud utilisés.

# Article 4 : Obligations du Sous-traitant

1. **Traitement conforme aux instructions** : Le Sous-traitant s’engage à ne traiter les données à caractère personnel que sur instruction documentée du Responsable de traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, sauf si une exigence légale l’y oblige.
2. **Confidentialité** : Le Sous-traitant doit veiller à ce que les personnes autorisées à traiter les données à caractère personnel s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
3. **Sécurité des traitements** : Le Sous-traitant s’engage à mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir la sécurité des données à caractère personnel qu’il traite, y compris celles traitées via des services cloud, conformément à l’article 32 du RGPD.
4. **Sous-traitance ultérieure** : Le Sous-traitant ne doit pas recourir à un autre sous-traitant sans l’autorisation préalable écrite et spécifique du Responsable de traitement. En cas de sous-traitance ultérieure autorisée, le Sous-traitant doit s’assurer que le sous-traitant ultérieur respecte les mêmes obligations de protection des données.
5. **Assistance au Responsable de traitement** : Le Sous-traitant doit assister le Responsable de traitement, dans la mesure du possible, pour s’acquitter de ses obligations en matière de sécurité des données, de notification des violations de données, de réalisation d’analyses d’impact sur la protection des données et de consultations préalables auprès des autorités de contrôle.
6. **Localisation des données** : Le Sous-traitant doit fournir des informations claires sur les lieux de stockage et de traitement des données dans les infrastructures cloud, et s’assurer que ces lieux respectent les réglementations applicables en matière de protection des données.

# Article 5 : Description des traitements

Le Sous-Traitant est autorisé à traiter pour le compte du Responsable de Traitement, les données à caractère personnel nécessaires pour fournir les Services. La nature et la catégorie des opérations réalisées sur les données à caractère personnel seront définies par le Responsable de Traitement selon les besoins spécifiques de chaque Service. Les finalités du traitement sont déterminées par le Responsable de Traitement et communiquées au Sous-Traitant. La nature et la catégorie des données à caractère personnel traitées sont spécifiées par le Responsable de Traitement. Les catégories de personnes concernées sont identifiées par le Responsable de Traitement. Pour l’exécution des Services, le Responsable de Traitement met à la disposition du Sous-Traitant les informations nécessaires. La durée du traitement est fixée par le Responsable de Traitement en fonction des exigences des Services fournis.

# Article 6 : Droits des personnes concernées

1. **Accès et rectification** : Le Responsable de traitement et le Sous-traitant doivent permettre aux personnes concernées d’exercer leurs droits d’accès et de rectification de leurs données à caractère personnel, conformément aux articles 15 et 16 du RGPD.
2. **Effacement et limitation du traitement** : Les personnes concernées doivent pouvoir exercer leurs droits à l’effacement de leurs données (droit à l’oubli) ou à la limitation du traitement, conformément aux articles 17 et 18 du RGPD.
3. **Portabilité des données** : Le Responsable de traitement doit assurer, lorsque cela est applicable, la portabilité des données à caractère personnel des personnes concernées, conformément à l’article 20 du RGPD.
4. **Opposition** : Les personnes concernées doivent pouvoir exercer leur droit d’opposition au traitement de leurs données personnelles conformément à l’article 21 du RGPD.

# Article 7 : Mesure de sécurité et de confidentialité

Le Sous-Traitant s’engage en particulier à mettre en place les mesures suffisantes pour assurer la sécurité et la confidentialité des Données Personnelles confiées et traitées dans le cadre des Services, à savoir notamment :

* Mettre en œuvre les mesures techniques et d’organisation appropriées pour protéger les Données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l’altération, l’utilisation détournée, la diffusion ou l’accès non autorisés, ainsi que contre toute autre forme de traitement illicite ;
* Ne pas utiliser les Données à caractère personnel pour son propre compte ou pour le compte de tiers et ne pas les transférer sans l’autorisation écrite et préalable du Responsable de Traitement ou du client final ;
* Veiller à ce que les personnes autorisées à traiter les Données à caractère personnel soient soumises à des obligations appropriées de confidentialités ;
* Ne pas réaliser de copies ou duplications des Données à caractère personnel sans l’autorisation écrite préalable du Responsable de Traitement ou du client final (à moins que cela soit nécessaire à l’accomplissement des Services fournis par le prestataire dans le cadre du Contrat) ;
* Informer le Responsable de Traitement de tout accès accidentel ou non autorisé aux Données à caractère personnel, de tout manquement à la réglementation sur les Données à caractère personnel ou toute suspicion d’un tel manquement, dans les meilleurs délais et, si possible, 48 heures au plus tard après en avoir pris connaissance.
* Selon le choix du Responsable de Traitement, supprimer ou renvoyer les Données à caractère personnel ou les renvoyer au terme du Contrat, et détruire les copies existantes, sauf obligation légale de les conserver ;
* Mettre en œuvre une politique de sécurité des systèmes d’information et de gestion des autorisations d’accès logique et physique notamment, qu’il devra maintenir et faire évoluer pendant toute la durée du Contrat.

# Article 8 : Notification des violations de données

En cas de violation de données à caractère personnel, le Sous-traitant doit notifier cette violation au Responsable de traitement sans délai indu après en avoir pris connaissance. Cette notification doit inclure toutes les informations pertinentes permettant au Responsable de traitement de notifier cette violation à l’autorité de contrôle compétente et, le cas échéant, aux personnes concernées conformément à l’article 33 du RGPD. La notification doit préciser l’impact potentiel sur les données hébergées dans le cloud et les mesures prises pour y remédier.

# Article 9 : Transferts de données hors de l’Union Européenne

Tout transfert de données à caractère personnel vers un pays tiers ou une organisation internationale ne peut être effectué que sous réserve du respect des conditions prévues par le RGPD, notamment aux articles 44 à 50. Le Responsable de traitement doit s’assurer que des garanties appropriées sont en place, telles que les clauses contractuelles types approuvées par la Commission européenne ou l’existence d’une décision d’adéquation.

# Article 10 : Durée et fin du traitement

À l’issue du contrat principal, le Sous-traitant s’engage, selon les instructions du Responsable de traitement, à supprimer toutes les données à caractère personnel ou à les retourner au Responsable de traitement, et à détruire les copies existantes sauf obligation légale contraire. Cette obligation inclut également les données stockées sur des supports de sauvegarde dans les infrastructures cloud, sauf si une obligation légale impose leur conservation.

# Article 11 : Documentation et audits

Le Sous-traitant mettra à la disposition du Responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues par la présente annexe et autorisera les audits, y compris les inspections, par le Responsable de traitement ou un autre auditeur mandaté par ce dernier, afin de vérifier la conformité avec cette annexe et le RGPD. Le Sous-traitant doit également tenir un registre des activités de traitement conformément à l’article 30 du RGPD et fournir des rapports de conformité sur les infrastructures cloud utilisées.

# Article 12 : Registre des activités de Traitement

Le Sous-traitant doit également tenir un registre des activités de Traitement conformément à l’article 30 du RGPD et fournir des rapports de conformité sur les infrastructures cloud utilisées. Ce registre contient à minima : - Le nom et coordonnées du responsable du traitement et, le cas échéant, du co-responsable du traitement, du représentant du responsable du traitement et du délégué à la protection des données ; - La description des catégories de personnes concernées et des catégories de données personnelles ; - Les finalités du Traitement ; - Les catégories de destinataires auxquels les données personnelles ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ; - La durée de conservation des données ; - La description générale des mesures techniques et organisationnelles de sécurité mises en œuvre.

Sur demande écrite du Responsable de Traitement, du client final ou de toute autorité compétente, le Sous-Traitant disposera d’un délai de 15 jours ouvrés pour communiquer une copie dudit registre à compter de la réception delate demande.

# Article 13 : Les sous-traitants ultérieurs

Le Sous-Traitant peut être amené à recourir à un (ou des) prestataire(s) / fournisseur(s) externes pour la prise en charge de prestations spécifiques relevant du Contrat. A cet effet, le Sous-traitant peut être amené à recruter, sous sa responsabilité, un (ou des) Sous-traitant(s) de second rang aux seules fins de fournir une partie des prestations nécessaires au système infogéré.

Le Sous-Traitant s’engage à conclure un acte juridique contraignant avec tout sous-traitant ultérieur qu’il engage pour le Traitement des Données, afin de lui imposer le respect des exigences du RGPD et les mêmes obligations que celles prévues par l’article 20.2. En particulier, le Sous-Traitant doit s’assurer que le sous-traitant ultérieur qu’il a recruté présente des garanties suffisantes pour la mise en œuvre des mesures de sécurité nécessaires.

En cas de défaillance du sous-traitant ultérieur dans le respect de ses obligations en matière de protection des Données personnelles, le Sous-traitant demeurera pleinement responsable à l’égard du Responsable de traitement, sans préjudice des droits des Personnes concernées prévus aux articles 79 et 82 du RGPD.

La liste des sous-traitants subséquents autorisés est la suivante:

1. Interxion
2. Data4
3. Telehouse
4. Iron Mountain

En cours d’exécution du Contrat, le Responsable de traitement peut accéder à tout moment auprès du Sous-Traitant à l’actualisation de ladite liste. Nonobstant ce qui précède, le Sous-traitant notifiera par écrit au Responsable de Traitement la liste des sous-traitants ultérieurs mise à jour régulièrement à l’exception d’un changement majeur de sous-traitant ultérieur.

# Article 14 : Responsabilité

Le Responsable de traitement et le Sous-traitant reconnaissent qu’ils peuvent être tenus pour responsables des dommages causés par un traitement des données à caractère personnel non conforme au RGPD et aux lois françaises applicables. Le Sous-traitant est responsable des dommages causés par le traitement s’il n’a pas respecté les obligations du RGPD spécifiquement applicables aux sous-traitants ou s’il a agi en dehors des instructions légales du Responsable de traitement ou contrairement à celles-ci.

# Article 15 : Modifications

Toute modification de la présente annexe doit faire l’objet d’un avenant écrit signé par les deux parties. Les modifications doivent être conformes aux exigences du RGPD et des lois françaises relatives à la protection des données personnelles.

# Article 16 : Loi applicable et juridiction compétente

La présente annexe est régie par le droit français. Tout litige relatif à son interprétation ou à son exécution sera de la compétence exclusive des tribunaux français. En cas de divergence entre les versions linguistiques de la présente annexe, la version française prévaudra.