# Annexe Contractuelle - Données à Caractère Personnel (DPA)

**Reference: Annexe - Données à Caractère Personnel**

**V2 - 17/10/2025 - Mise à jour conformité CISPE**

## Article 1 : Définitions

**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).

**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.

**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.

**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.

**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.

**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.

**Service Cloud**: Tout service de traitement, stockage, ou gestion de données à caractère personnel fourni par le Sous-traitant via des infrastructures cloud.

**Accès nécessaire au service**: Tout accès aux données à caractère personnel strictement requis pour l'exécution des services contractuels définis, incluant la fourniture, la maintenance, le support technique, la supervision des systèmes, et la résolution d'incidents, à l'exclusion de tout accès à des fins d'analyse commerciale, de profilage, ou de marketing direct.

## 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, ainsi qu'aux exigences du code de conduite CISPE.

## Article 3 : Obligations du Responsable de traitement

- **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.

- **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.

- **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.

- **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.

- **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

### 4.1 Traitement conforme aux instructions et limitation des accès

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.

- Limiter strictement ses accès aux données à caractère personnel aux seuls **accès nécessaires au service** tels que définis à l'Article 1.

- **S'interdire formellement** tout traitement des données à caractère personnel à des fins de:

- Data mining ou exploration de données.

- Profilage des utilisateurs finaux ou analyse comportementale.

- Marketing direct ou publicité ciblée.

- Toute utilisation commerciale non liée à l'exécution des services contractuels.

### 4.2 Politique de gestion des accès

Le Sous-traitant maintient une politique détaillée de gestion des accès aux données clients qui inclut :

- Les procédures d'autorisation et de révocation des accès.

- L'identification des personnes habilitées et leurs niveaux d'accès.

- Les contrôles d'accès physiques et techniques aux infrastructures.

- La journalisation complète des accès avec conservation sur 24 mois minimum.

- Les procédures de gestion des accès d'urgence et de supervision.

### 4.3 Obligations générales

- **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.

- **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.

- **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.

- **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.