ANNEXE « PROTECTION DES DONNEES A CARACTERE PERSONNEL »

La présente annexe a pour objet de définir les conditions dans lesquelles le titulaire est autorisé à traiter des données à caractère personnel pour le compte du Musée National Picasso Paris (MNPP), dans le cadre de l'exécution des prestations objet du présent accord-cadre. Elle précise les droits et obligations respectifs des parties au regard de la réglementation applicable en matière de protection des données à caractère personnel, et notamment du règlement (UE) 2016/679 du 27 avril 2016 (RGPD).

Elle s'applique aux seuls traitements de données à caractère personnel réalisés par le Titulaire pour le compte du Musée National Picasso Paris, tels que décrits en Annexe A.

1. Définitions

- « Législation relative à la protection des Données à caractère personnel » désigne le Règlement (UE) 2016/679 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, abrogeant la directive 95/46/CE (« Règlement général sur la protection des Données » ou « RGPD »), la Loi Informatique et Libertés n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par l'ordonnance n°2018-1125 du 12 décembre 2018, ainsi que toute disposition légale ou règlementaire en vigueur à la date de signature du contrat concernant la protection des données à caractère personnel.

- « Données à caractère personnel », « Traitement », « Responsable du Traitement », « Sous-traitant/Sous-traitance », « Personne concernée », « Finalité de traitement », « Autorité de contrôle », « Analyse d'Impact relative à la Protection des Données (AIPD) », « Registre des activités de Traitement », « Violations de Données», « Protection des Données dès la conception », « Protection des données par défaut », « Clauses Contractuelles Types » ont la même signification que dans la Législation relative à la protection des Données à caractère personnel.

- « Documentation relative aux traitements » désigne l'ensemble de la documentation dont la tenue permet de démontrer la conformité à la Législation relative à la protection des données personnelles.

- « Opérations de traitement autorisées » désigne les opérations de traitement que le Musée National Picasso Paris autorise à l'annexe A.

2. Rôles et responsabilité

Pour la fourniture des Prestations définies au cahier des charges, il est convenu entre les Parties que le Musée National Picasso Paris a la qualité de Responsable du Traitement et le Titulaire celle de Sous-traitant intervenant pour le compte du Musée National Picasso Paris au sens du RGPD, pour les seuls traitements décrits en Annexe A.

Toutefois, pour les traitements de données à caractère personnel mis en œuvre par le Titulaire pour ses propres finalités, notamment lorsqu'ils résultent d'obligations légales ou réglementaires qui lui sont applicables, le Titulaire agit en qualité de responsable de traitement distinct.

Par ailleurs, lorsque l'exécution du Contrat entraine la communication par l'une des Parties à l'autre Partie de Données à caractère personnel relatives aux contacts professionnels ou aux intervenants dans le cadre de l'exécution du Contrat, les Parties reconnaissent qu'elles ont chacune la qualité de responsables de traitement indépendants pour le traitement des Données à caractère personnel communiquées. Les Données à caractère personnel sont susceptibles d'être traitées par la Partie qui les reçoit à des fins de gestion de la relation commerciale, de communication institutionnelle, de fourniture des Prestations, ou pour toutes autres finalités légitimes décrites dans les notices et / ou politiques de protection des données à caractère personnel de la Partie recevant lesdites données.

3. Obligations générales des Parties

Les Parties déclarent connaître les droits et obligations incombant respectivement aux Responsables du traitement et aux Sous-Traitants résultant de l'application de la Législation relative à la protection des données à caractère personnel et s'engagent à les respecter.

Les Parties s'engagent à collaborer activement afin de permettre le respect par chacune d'elle des droits et obligations résultant de l'application de la Législation relative à la protection des Données à caractère personnel.

4. Instructions du Musée National Picasso Paris lorsque le Titulaire agit en qualité de Sous-traitant

Le détail des opérations de Traitement de Données à caractère personnel confiées au Titulaire (Finalités de traitement, Opérations de traitement Autorisées, catégories de données à caractère personnel, catégories de personnes concernées, durée de conservation, mesures de sécurité à mettre en œuvre dans le cadre de la prestation) sont décrites à l'annexe A.

Les Données à caractère personnel ne pourront être traitées que dans le cadre des Finalités de traitement et des Opérations de traitement Autorisées et décrites à l'annexe A ou ayant donné lieu à une instruction écrite du Musée National Picasso Paris et ce, uniquement par le Titulaire, les Sous-traitants ultérieurs ou de toute personne agissant sous l'autorité du Titulaire.

En conséquence, le Titulaire s'engage à s'assurer, par tous moyens appropriés, que ses employés et, le cas échéant, ceux de ses Sous-traitants (ci-après, ensemble, les « Personnes Autorisées ») ne traitent les Données à caractère personnel que dans la limite nécessaire aux Finalités de traitement décrites par le Musée National Picasso Paris en annexe A et selon les Opérations de traitement Autorisées.

Pour éviter toute ambiguïté, le Titulaire s'engage à :

- S'abstenir de tout traitement de Données à caractère personnel non conforme aux instructions écrites du Musée National Picasso Paris ou étranger à l'exécution du présent Contrat, et notamment de tout usage personnel ;
- Obtenir l'autorisation préalable du Musée National Picasso Paris pour toute utilisation des Données à caractère personnel à des fins statistiques ou d'études, y compris lorsque celles-ci sont réalisées de manière pseudonyme ou anonyme ;

- Ne prendre aucune copie des documents et supports d'informations comportant des Données à caractère personnel qui lui sont confiés, à l'exception de celles nécessaires à l'exécution du Contrat, sans avoir recueilli l'accord préalable écrit du Musée National Picasso Paris.

Les Données à caractère personnel ne pourront faire l'objet d'aucune divulgation ou communication à des tiers en dehors des cas expressément prévus dans le Contrat ou résultant des instructions écrites du Musée National Picasso Paris ou de ceux prévus par une disposition légale ou réglementaire.

Le Titulaire alerte le Musée National Picasso Paris par courrier électronique avec accusé de réception au responsable de l'accord-cadre dans un délai de 5 jours, s'il considère qu'une de ses instructions constitue une violation de la Législation relative à la protection des Données à caractère personnel.

5. Demandes de droits des personnes concernées et demande de communication des Tiers autorisés

Le Titulaire aide, dans la mesure du possible, le Musée National Picasso Paris à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées et des demandes de communication de documents ou de renseignements contenant des Données à caractère personnel qui émaneraient de tiers se prélavant d'autorisation découlant de l'application de dispositions légales ou réglementaires (« Tiers autorisés »), sauf dans les cas où cette information est interdite du fait des dispositifs légaux et réglementaires applicables.

Le Titulaire notifie dès réception les demandes qui lui sont adressées au Musée National Picasso Paris par courrier électronique avec accusé de réception au responsable de l'accord-cadre

Le Titulaire ne procède à aucune communication sans avoir reçu les instructions préalables du Musée National Picasso Paris.

Le Titulaire s'engage à satisfaire par écrit aux demandes d'information du Musée National Picasso Paris dans un délai de cinq jours ouvrés à compter de la demande, afin de lui permettre de répondre aux demandes d'exercice des droits présentées par les personnes concernées par les Traitements et les demandes de communication des Tiers autorisés.

6. Sécurité et confidentialité des Traitements

Le Titulaire s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles tenant compte des règles de l'art et des standards de sécurité destinées à assurer la sécurité des Données à caractère personnel. Plus exactement le Titulaire met en œuvre les mesures de sécurité qui sont appropriées au regard des Finalités de traitement et des Opérations de traitement Autorisées, du contexte, de la portée et des risques générés par le Traitement pour les personnes concernées, ainsi qu'à prévenir les Violation de données. Ces mesures devront *a minima* comprendre ou mettre en œuvre les mesures ou objectifs de sécurité visés en annexe A.

Le Titulaire s'engage à mettre en œuvre des procédures assurant que les tiers qu'il autorise à accéder aux Données à caractère personnel, y compris ses propres Sous-traitants, respectent et préservent la confidentialité et la sécurité des Données à caractère personnel. Le Titulaire s'assure que toute Personne Autorisée soit tenue par une obligation de confidentialité résultant d'un engagement écrit ou d'une obligation légale.
Le Titulaire s'engage à ne pas utiliser de Données à caractère personnel dans les environnements de test ou de développement, sauf autorisation express et écrite du Musée National Picasso Paris. Dans ce cas, les Données à caractère personnel devront être pseudonymisées.

Le Titulaire s'engage à notifier par courrier électronique avec accusé de réception à l'adresse courriel du responsable de l'accord-cadre au Musée National Picasso Paris tout changement significatif susceptible d'affecter la sécurité ou la conformité du Traitement (modification d'architecture, transfert d'hébergement, mise à jour majeure, etc.), et, ce, dans un délai de cinq jours à compter dudit changement.

Le Titulaire devra mettre en œuvre toutes mesures additionnelles appropriées résultant de l'application de la Législation relative à la protection des données personnelles et/ou de l'AIPD conduite en application du Contrat.

Les mesures mises en œuvre au titre du présent article devront notamment, et sans préjudice des autres mesures applicables, viser à :

- Assurer le traitement des Données à caractère personnel de manière séparée des propres Données du Titulaire ou de Données d'autres clients ou fournisseurs du Titulaire ;
- Empêcher, d'une part, tout accès non autorisé aux Données ou toute utilisation non conforme aux Finalités de traitement et aux Opérations de traitement Autorisées et décrites en annexe A, de manière accidentelle ou illicite, et, d'autre part, toute destruction, perte, altération, divulgation non autorisée de Données à caractère personnel que ce soit ; lors de la conservation, la transmission ou toute autre forme de Traitement ;
- Assurer la détection des Violations de données ;
- Assurer la traçabilité des connexions aux Données à caractère personnel traitées dans le cadre de l'exécution du Contrat pour une durée minium de six (6) mois ;
- Garantir la confidentialité des données (chiffrement, pseudonymisation, …) ;
- Garantir l'intégrité, la disponibilité et la résilience des systèmes et des Services, tenant compte des objectifs de sécurité visés aux annexes A et B ;
- Garantir que les outils, plateformes ou logiciels mis à disposition respectent les principes de Privacy by design et Privacy by default et qu'ils permettent la journalisation, la suppression et l'anonymisation des Données à caractère personnel, l'export des Données à caractère personnel dans un format structuré ;
- Tenir à jour une documentation écrite décrivant les mesures de sécurité techniques et organisationnelles ainsi mises en œuvre ;
- Maintenir un plan de continuité et de reprise d'activité incluant les situations de compromission de données en cas d'incident technique ou physique, et, ainsi, rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans les délais appropriés ;
- Tester, analyser et évaluer régulièrement, et au moins une fois par an, l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement, et en justifier auprès du Musée National Picasso Paris ;
- Garantir que l'accès et la consultation des Données à caractère personnel traitées sont limités aux seuls personnels dûment habilités et autorisés, dans la stricte limite de ce qui leur est nécessaire à l'accomplissement de leurs fonctions ;
- Tenir à jour la liste des personnes autorisées à avoir accès aux Données à caractère personnel et la communiquer au Musée National Picasso Paris en cas de demande ;
- Garantir la destruction des Données à caractère personnel à la fin de la durée de conservation telle que définie au présent Contrat.

Le Titulaire met en œuvre, en concertation avec le Musée National Picasso Paris, des procédés (adoption d'une politique de gouvernance des données, anonymisation des données non nécessaires…), destinés à assurer que seules les Données strictement nécessaires aux Finalités de traitement sont traitées dans le cadre de l'exécution du Contrat, et, ce, conformément aux Opérations de traitement Autorisées.

Le Titulaire fait réaliser des tests, contrôles et audits réguliers de son système d'information afin de contrôler le respect de la mise en œuvre des mesures techniques et organisationnelles détaillées aux annexes A et B. Il justifie de ces contrôles au Musée National Picasso Paris et lui fournit les conclusions de ces tests, contrôles et audits.

7. Notification des violations de Données à caractère personnel

Le Titulaire notifie au Musée National Picasso Paris toute violation de Données à caractère personnel dans les meilleurs délais et au plus tard dans un délai de 24h après en avoir pris connaissance. A cet effet, le Titulaire documente une procédure permettant la détection, la résolution et la notification dans les plus brefs délais des violations de Données à caractère personnel.

Les notifications sont effectuées en adressant un courrier électronique avec avis de réception aux adresses suivantes :

- cnil@museepicassoparis.fr

hicham.bouchiki@museepicassoparis.fr

Les notifications sont accompagnées de toute documentation utile afin de permettre au Musée National Picasso Paris, si nécessaire, de notifier cette violation à la CNIL.

La notification contient, dans la limite des informations portées à la connaissance du Titulaire :

- la description de la nature de la Violation de Données y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact du Titulaire auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la Violation de Données ;
- la description des mesures prises pour remédier à la Violation de Données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

8. Sous-traitance ultérieure de Traitement de Données à caractère personnel

Le Titulaire complète en annexe B la liste des Sous-traitants ultérieurs auxquels il recourt. Celle-ci doit faire l'objet d'une validation écrite du Musée National Picasso Paris.

Tout recours par le Titulaire à un Sous-traitant ultérieur impliquant un Traitement de Données à caractère personnel durant l'exécution du Contrat devra également avoir été préalablement et spécifiquement autorisé par écrit par le Musée National Picasso Paris (notamment lorsque cela le nécessite, via le formulaire DC4 disponible sur le site https://www.economie.gouv.fr/daj/formulaires-declaration-du-Titulaire).

En l'absence d'une telle autorisation, le Titulaire n'est pas autorisé à transférer des Données à caractère personnel à un Sous-traitant ultérieur.

Le Titulaire s'engage à reporter sur ses Sous-traitants ultérieurs l'ensemble des obligations figurant au présent Contrat, et en particulier à mettre à la charge de ses Sous-traitants ultérieurs toutes obligations nécessaires pour que soient respectées la confidentialité, la sécurité, la disponibilité et l'intégrité des Données à caractère personnel, et pour que lesdites données ne puissent être ni cédées ou louées à un tiers à titre gratuit ou non, ni utilisées à d'autres fins que celles définies au présent Contrat.

Le Titulaire demeure pleinement responsable de l'exécution des obligations du Contrat par ses propres Sous-traitants ultérieurs et vérifie régulièrement, notamment par des contrôles et audits, tels que visés à l'article 6, le respect de leurs obligations.

Le Titulaire tient à jour la liste comportant : le nom et coordonnées de ses éventuels Sous-traitants ultérieurs ainsi que la nature des opérations confiées, l'identification des lieux de Traitements, la nature des opérations confiées et la date des derniers audits réalisés.

9. Transferts de Données en dehors de l'Union Européenne (UE)

Le Titulaire s'engage à héberger et traiter les Données à caractère personnel exclusivement sur le territoire d'un État membre de l'Union Européenne.

Le Titulaire s'assure qu'aucune Donnée à caractère personnel n'est transférée en dehors de l'Espace économique européen par ses propres Sous-traitants.

Par dérogation à ce qui précède, le Titulaire est autorisé, dans la stricte limite nécessaire à l'exécution de la Prestation, à recourir à des Prestataires ou des moyens de Traitement situés dans un État en dehors de l'Union Européenne pour les opérations de Traitements préalablement autorisées à l'annexe A ou celles pour lesquelles le Titulaire aura reçu l'autorisation écrite, expresse et spécifique du Musée National Picasso Paris sous réserve que :

- Le transfert ait lieu vers un pays tiers bénéficiant d'une décision d'adéquation au sens de la Législation relative à la protection des Données à caractère personnel (article 45 RGPD), ou que ;
- Les transferts soient encadrés par la conclusion de Clauses Contractuelles Types selon les modalités prévues par décision de la Commission Européenne, pour le transfert de Données à caractère personnel vers des Sous-traitants établis dans des pays tiers, le Titulaire se portant fort de la signature et du respect des Clauses Contractuelles Types par ses propres Sous-traitants et s'engageant à notifier sans délai par courrier électronique avec accusé de réception au Musée National Picasso Paris la copie des Clauses Contractuelles Types en application du présent paragraphe, ou que ;

- Les transferts soient fondés sur l'adoption par le Titulaire de Règles d'entreprise contraignantes (article 47 RGPD) annexées au présent Contrat reconnues conformes par l'Autorité de contrôle compétente.

Les pays situés en dehors de l'Union Européenne vers lesquels sont transférés des Données à caractère personnel, ainsi que les modalités desdits transferts, sont précisés en annexe B.

10. Sort des données et réversibilité technique

Au terme du Contrat, le Titulaire s'engage à restituer de manière systématique, dans un format interopérable, l'ensemble des Données à caractère personnel traitées pour le compte du Musée National Picasso Paris et, le cas échéant, à s'assurer que les sous-traitants du Titulaire fassent de même.

Le Titulaire s'engage également à restituer l'ensemble des logs, métadonnées et éléments techniques nécessaires dans un format structuré, lisible, interopérable et ouvert. Il accompagne techniquement l'opération.

Le Titulaire garantit la destruction sécurisée des données restantes, avec attestation écrite.

Cette obligation demeure applicable même après la fin du Contrat quelle qu'en soit la raison.

11. Contrôle et Audit

Sans préjudice des obligations du Sous-traitant telles que visées au paragraphe 6 du présent Contrat, le Musée National Picasso Paris se réserve le droit de procéder à tout contrôle et vérification, y compris auprès des Sous-traitants ultérieurs du Titulaire, permettant d'évaluer le respect par le Titulaire des obligations prévues dans la présente clause.

Le Titulaire autorise expressément le Musée National Picasso Paris (ou un auditeur mandaté par ses soins) à accéder aux locaux et installations (du Titulaire ou de ses Sous-traitants ultérieurs) consacrés au Traitement de Données à caractère personnel en exécution du Contrat aux fins de réaliser ou faire réaliser un audit. Ces audits ont pour objet de vérifier notamment que les règles relatives à la protection des Données à caractère personnel et les procédures de confidentialité et de sécurité prévues au contrat sont respectées. Le Musée National Picasso Paris notifie par courrier électronique avec accusé de réception son intention au Titulaire, dans un délai raisonnable, de procéder à un tel audit durant des heures d'ouverture. Le Musée National Picasso Paris s'engage à ne pas perturber de manière déraisonnable les activités du Titulaire et de ses Sous-traitants ultérieurs.

Le Titulaire met à la disposition du Musée National Picasso Paris la Documentation relative aux Traitements, ainsi que toutes autres informations nécessaires ou utiles afin, d'une part, de démontrer le respect de la Législation relative à la protection des données à caractère personnel, comme la tenue du Registre des activités de sous-traitance, et, d'autre part, de permettre la réalisation d'audits par le Musée National Picasso Paris ou par tout organisme tiers qu'il aurait mandaté.

Dans l'hypothèse où le rapport d'audit ferait apparaître un manquement du Titulaire à ses obligations, le Titulaire devra mettre en œuvre les mesures correctives jugées nécessaires par le Musée National Picasso Paris selon un calendrier convenu entre les Parties. À défaut de voir le Titulaire remédier en temps voulu aux manquements constatés, le Musée National Picasso Paris pourra, selon les cas, prononcer des pénalités ou résilier de plein droit le Contrat sans préavis, sans préjudice des dommages et intérêts auxquels le Titulaire pourrait prétendre.

12. Registre des catégories d'activités de traitement

Le Titulaire s'engage à tenir par écrit un registre de toutes les activités de traitement effectuées pour le compte du Responsable du traitement conformément à l'article 30.2 du RGPD.

Le Titulaire tient le registre à la disposition de l'autorité de contrôle et du Musée National Picasso Paris sur demande.

13. Délégué à la protection des données

Le Musée National Picasso Paris a désigné un délégué à la protection des données dont les coordonnées sont les suivantes :

- Adresse de courriel : cnil@museepicassoparis.fr

Le Titulaire communique au Musée National Picasso Paris le nom et les coordonnées de son délégué à la protection des données (Annexe B), s'il en a désigné un conformément à l'article 37 du RGPD.

14. Collaboration et assistance

Le Titulaire s'engage à communiquer au Musée National Picasso Paris toute information requise ou utile pour lui permettre de tenir à jour la Documentation relative aux Traitements, pour démontrer sa conformité à la Législation relative à la protection des Données à caractère personnel, ou pour répondre aux demandes présentées par les Autorités de protection des données ou le délégué à la protection des Données du Musée National Picasso Paris.

Le Titulaire conseille et assiste le Musée National Picasso Paris dans la conduite des AIPD, la mise en œuvre de mesures de Protection des Données à caractère personnel dès la conception et de Protection des Données à caractère personnel par défaut, ainsi que le cas échéant en vue de l'accomplissement des formalités préalables obligatoires auprès de l'Autorité de contrôle ou de toute autre autorité.

Le Titulaire assiste sans frais le Musée National Picasso Paris afin de lui permettre de répondre selon les modalités et dans les délais requis par la Législation relative à la protection des données personnelles :

- Aux demandes d'exercice de droits des personnes concernées (dans les conditions visées au paragraphe 5)

- Aux demandes présentées par la CNIL.

15. Engagements du Musée National Picasso Paris

Le Musée National Picasso Paris s'engage, pour sa part :

- A ne transmettre au Titulaire que les Données à caractère personnel strictement nécessaires à l'exécution de ses obligations contractuelles ;

- A formuler ses instructions au Titulaire s'agissant d'un Traitement de Données à caractère personnel par écrit ;

- A garantir le respect des droits relatifs à la protection des Données à caractère personnel des personnes concernées et notamment, le cas échéant, le droit d'être tenu informé de la communication de leurs Données au Titulaire ;

- A veiller pendant toute la durée des Traitements de Données à caractère personnel sur lesquels le Titulaire pourrait être conduit à intervenir au respect des obligations prévues par la Législation relative à la Protection des Données à caractère personnel.

16. **Responsabilité**

Nonobstant toutes dispositions contenues dans le présent Marché, les Parties conviennent expressément que :

- La responsabilité du Titulaire pour tout manquement à l'une quelconque de ses obligations en vertu de la Législation relative à la protection des données personnelles ou de la présente clause ne saurait être limitée financièrement ; et

- La perte de Données à caractère personnel est exclue de toute qualification éventuelle de dommages indirects.

- **Annexe – Description des mesures de sécurité mises en œuvre par le Candidat**

- Description des mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque mises en œuvre par le Candidat ;

- Liste des Sous-traitants ultérieurs ;

- Description des transferts de Données en dehors de l'Union Européenne ;

- Liste des points de contacts chez le Sous-Traitant.