

MARCHÉ DE SERVICES N° AO-2025-09

Services d'Assurances pour

CITE DE L'ARCHITECTURE ET DU PATRIMOINE

Lot 3 – Auto-Mission

ANNEXE 2 de l'acte d'engagement
« Charte de sous-traitance et protection des données personnelles »

La Cité de l'architecture et du patrimoine, responsable du traitement, rappelle à la société Titulaire du marché le caractère stratégique et strictement confidentiel de toutes les données à caractère personnel.

Aussi, le Titulaire reconnaît que l'ensemble des données et fichiers communiqués par la Cité de l'architecture et du patrimoine relève de la vie privée et du secret professionnel et est soumis :

- À la loi relative à l'informatique, aux fichiers et aux libertés n° 78-17 du 6 janvier 1978 modifiée et ses éventuelles mises à jour ;
- Au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données) abrogeant la Directive 95/46/CE, applicable à partir du 25 mai 2018 ;
- Aux textes et décisions émanant d'autorités de contrôle, notamment de la Commission nationale de l'Informatique et des Libertés (Cnil) ;

Le Titulaire garantit à la Cité de l'architecture et du patrimoine le respect des obligations légales et réglementaires lui incombant et le respect de ses obligations au titre de la présente Charte.

Le Titulaire s'engage à mettre en place toutes les procédures nécessaires pour en assurer la confidentialité et la plus grande sécurité et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte du responsable de traitement (la Cité de l'architecture et du patrimoine) les opérations de traitement de données à caractère personnel définies ci-après.

1. Description des traitements

Le Titulaire sera amené à traiter des données à caractère personnel dans le cadre des traitements décrits ci-après. La Cité de l'architecture et du patrimoine, pourra modifier à tout moment la description de ces traitements et en notifiera le Titulaire.

1.1 - Objet des traitements

Le marché a pour objet la réalisation de prestations d'assurance « Auto-Mission ».

1.2 - Durée

La durée des traitements est égale à la durée du marché.

1.3 - Nature et finalité des traitements

La finalité du traitement est la bonne gestion des données à caractère personnel de la Cité de l'architecture et du patrimoine dans la cadre d'exécution du marché cité en objet.

Les données à caractère personnel qui pourront être traitées sont les noms, coordonnées téléphoniques et mail des salariés, et collaborateur de la Cité de l'architecture et du patrimoine.

Les données à caractère personnel concernent également : les noms, coordonnées téléphoniques et mail des réservataire et visiteurs de la Cité de l'architecture et du patrimoine.

2. Obligations du sous-traitant

Le Titulaire s'engage à prendre toutes les mesures nécessaires au respect par lui-même et par son personnel de ses obligations et notamment à :

- traiter les données conformément aux instructions documentées du responsable de traitement. Si le titulaire considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le titulaire est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union

ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :

- S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
- Reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut ;

- prendre toute mesure permettant d'empêcher toute utilisation détournée, malveillante ou frauduleuse des données et des fichiers ;

- notifier immédiatement à la Cité de l'architecture et du patrimoine toute modification ou changement pouvant impacter le traitement des données à caractère personnel ;

Les parties conviennent de définir la notion d'instruction comme étant acquise lorsque le Titulaire agit dans le cadre de l'exécution des présentes et du Marché.

Le Titulaire s'engage à prendre toute mesure utile afin de garantir que les personnes physiques agissant sous son autorité et ayant accès aux données à caractère personnel ne les traite pas, excepté sur instruction de la Cité de l'architecture et du patrimoine, à moins d'y être obligé par une disposition impérative résultant du droit communautaire ou du droit d'un Etat membre de l'Union européenne applicable aux traitements objet des présentes. Le Titulaire veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité des données ou soient soumises à une obligation légale appropriée de confidentialité.

Par ailleurs, le Titulaire s'interdit :

- de traiter, consulter les données ou les fichiers à d'autres fins que l'exécution des prestations qu'il effectue pour la Cité de l'architecture et du patrimoine au titre des présentes ;

- consulter, traiter les données autres que celles concernées par les présentes et ce, même si l'accès à ces données est techniquement possible ;

- de divulguer, sous quelque forme que ce soit, tout ou partie des données exploitées ;

- de prendre copie ou de stocker, quelles qu'en soient la forme et la finalité, tout ou partie des informations ou données contenues sur les supports ou documents qui lui ont été confiés ou recueillies par elle au cours de l'exécution des présentes, en dehors des cas couverts par les présentes.

- d'insérer dans les fichiers des données étrangères ;

- d'effectuer des études statistiques sur les données ou de traitement autre que celui demandé par la Cité de l'architecture et du patrimoine.

Le Titulaire reconnaît et accepte qu'il ne peut agir en matière de traitement des données et des fichiers auxquels il peut avoir accès que conformément aux présentes et au Marché.

3. Sous-traitance

Le Titulaire peut faire appel à un sous-traitant au sens de la réglementation Informatique et libertés pour sous-traiter tout ou partie des prestations. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance et le pays dans lequel s'opère la sous-traitance notamment s'il sous-traite vers un pays qui n'est pas situé dans l'Union européenne. Le responsable de traitement dispose d'un délai minimum de 1 mois à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Dans l'hypothèse où le Titulaire aurait été autorisée, le cas échéant tacitement, à sous-traiter les prestations objet du Marché, il s'engage à :

- informer et signer avec son sous-traitant ultérieur un contrat écrit faisant référence au Marché et à la présente Charte, et imposant au sous-traitant les mêmes obligations en matière de protection des données que celles fixées dans la présente Charte et au Marché ;
- mettre à la charge de son sous-traitant toutes obligations nécessaires pour que soient respectées la confidentialité, la sécurité et l'intégrité des données, 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 dans la présente Charte et au Marché ;
- communiquer à la Cité de l'architecture et du patrimoine une copie du contrat avec son ou ses sous-traitants et à défaut une description des éléments essentiels du contrat, incluant la mise en œuvre des obligations relatives à la protection des données à caractère personnel ;
- en cas d'autorisation écrite générale, informer la Cité de l'architecture et du patrimoine de toute modification prévue concernant l'ajout ou le remplacement d'autres sous-traitants, afin de permettre à la Cité de l'architecture et du patrimoine, le cas échéant, d'émettre des objections à l'encontre de ces changements.
- tenir à la disposition de la Cité de l'architecture et du patrimoine une liste du ou des sous-traitants impliqués dans le traitement de données à caractère personnel.

Les données traitées en exécution du Marché ne pourront faire l'objet d'aucune divulgation à des tiers, et ce y compris aux sous-traitants du Titulaire, en dehors des cas prévus dans la présente Charte et dans le Marché ou de ceux prévus par une disposition légale ou réglementaire.

Lorsque ses sous-traitants ne remplissent pas leurs obligations en matière de protection des données, le Titulaire demeure pleinement responsable devant la Cité de l'architecture et du patrimoine de l'exécution par les sous-traitants de leurs obligations.

4 Sécurité

Le titulaire s'engage à mettre en œuvre toutes les mesures de sécurité comme par exemple :

- La pseudonymisation et le chiffrement des données à caractère personnel
- Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- Les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

Le Titulaire s'engage également et conformément à la réglementation Informatique et Libertés, à prendre toutes précautions utiles au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données des fichiers et notamment empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès par des tiers non autorisés préalablement.

Il met en œuvre toutes mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

Le Titulaire s'engage à maintenir ces moyens tout au long de l'exécution du Marché et à défaut, à en informer immédiatement la Cité de l'architecture et du patrimoine.

En tout état de cause, le Titulaire s'engage en cas de changement des moyens visant à assurer la sécurité et la confidentialité des données et des fichiers, à les remplacer par des moyens d'une performance supérieure. Aucune évolution ne pourra conduire à une régression du niveau de sécurité.

5. Violation de données

Le Titulaire s'engage à notifier à la Cité de l'architecture et du patrimoine, dans les meilleurs délais et au plus tard 48 heures maximum, après en avoir pris connaissance, toute violation de donnée à caractère personnel, soit toute 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 traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Cette notification est accompagnée de toute documentation utile.

Après accord du responsable de traitement, le titulaire notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus

tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- La description de la nature de la violation de données à caractère personnel 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 auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données à caractère personnel ;
- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, 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.

Après accord du responsable de traitement, le titulaire communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- La description de la nature de la violation de données à caractère personnel 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 auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données à caractère personnel ;
- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lors d'une violation de données, le Titulaire s'engage à procéder à toutes investigations utiles sur les manquements aux règles de protection afin d'y remédier dès que possible et de diminuer l'impact de tels manquements sur les personnes concernées. Le Titulaire s'engage à informer la Cité de l'architecture et du patrimoine de ses investigations et ce de manière régulière.

Le Titulaire s'engage à collaborer activement avec la Cité de l'architecture et du patrimoine pour qu'ils soient en mesure de répondre à leurs obligations réglementaires et contractuelles.

6. Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

7. Exercice des droits des personnes

Dans la mesure du possible, le titulaire doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Ainsi, le Titulaire coopère notamment à la gestion des demandes des personnes concernées par les traitements tendant à l'exercice de leurs droits et notamment de leur droit d'accès aux données qui les concernent. Si une personne concernée devait contacter directement le Titulaire pour exercer ses droits d'accès, de rectification, de suppression et/ou d'opposition ou pour toute autre demande liée à la protection des données à caractère personnel, le Titulaire communiquera à la Cité de l'architecture et du patrimoine dans un délai de 72 heures maximum les demandes qui lui seront parvenues.

Le titulaire doit répondre sur instruction de la Cité de l'architecture et du patrimoine, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

8. Flux transfrontières de données

En cas de transfert de données à caractère personnel vers un pays tiers, n'appartenant pas à l'Union européenne, ou vers une organisation internationale, le Titulaire devra obtenir l'accord préalable écrit de la Cité de l'architecture et du patrimoine. Si cet accord est donné, le Titulaire s'engage à coopérer avec la Cité de l'architecture et du patrimoine afin d'assurer :

- le respect des procédures permettant de se conformer à la réglementation Informatique et libertés, par exemple dans le cas où une autorisation de la part de la Cnil apparaîtrait nécessaire ;
- si besoin, la conclusion d'un ou plusieurs contrats permettant d'encadrer les flux transfrontières de données. Le Titulaire s'engage en particulier, si nécessaire, à signer de tels contrats avec la Cité de l'architecture et du patrimoine et/ou à obtenir la conclusion de tels contrats par ses sous-traitants ultérieurs. Pour ce faire, il est convenu entre les Parties que les clauses contractuelles types publiées par la Commission européenne seront utilisées pour encadrer les flux transfrontières de données.

9. Tenue du registre

Le Titulaire, en tant que sous-traitant, s'engage à tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, conformément aux dispositions du règlement général sur la protection des données.

Ce registre comprend :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour le compte du responsable du traitement ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - La pseudonymisation et le chiffrement des données à caractère personnel ;
 - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
 - Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le Titulaire donnera à la Cité de l'architecture et du patrimoine accès au registre sur demande.

10. Conservation des données

Au terme du Marché, le Titulaire s'engage à restituer les fichiers et données à la Cité de l'architecture et du patrimoine dans les conditions spécifiées par la Cité de l'architecture et du patrimoine puis à détruire tous fichiers manuels ou informatisés stockant les informations collectées, sauf disposition impérative contraire résultant du droit communautaire ou du droit d'un Etat membre de l'Union européenne applicable aux traitements objets des présentes.

Dans l'hypothèse où le droit communautaire ou le droit d'un Etat membre exigerait la conservation des données à caractère personnel, le Titulaire informera la Cité de l'architecture et du patrimoine de cette obligation.

Le Titulaire s'engage à fournir à la Cité de l'architecture et du patrimoine, à première demande, un certificat de suppression des données à caractère personnel.

11. Documentation & vérifications

Le titulaire met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

La Cité de l'architecture et du patrimoine se réserve ainsi le droit de procéder à toutes vérifications qui lui paraissent utiles pour constater le respect des obligations précitées, et notamment en procédant à un audit de sécurité auprès du Titulaire ou directement auprès d'un sous-traitant ultérieur.

Par conséquent, le Titulaire s'engage à répondre aux demandes d'audit de la Cité de l'architecture et du patrimoine effectuées par elle-même ou par un tiers de confiance qu'elle aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Titulaire, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à la Cité de l'architecture et du patrimoine.

Les audits doivent permettre une analyse du respect par le Titulaire de ses obligations au titre de la présente Charte et du Marché, ainsi qu'au titre de la réglementation Informatique et libertés. Ils doivent permettre notamment de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

Enfin, le responsable de traitement s'engage à :

- Fournir au titulaire les données nécessaires à l'exécution de son contrat
- Documenter par écrit toute instruction concernant le traitement des données par le titulaire
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du titulaire
- Superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire

12. Délégué à la protection des données

Le titulaire communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

En cas de changement dans la personne du délégué à la protection des données, le Titulaire en informe sous 15 jours la Cité de l'architecture et du patrimoine.

13. Coopération

Le Titulaire s'engage à coopérer avec la Cité de l'architecture et du patrimoine:

- afin de permettre la réalisation de toute analyse d'impact que la Cité de l'architecture et du patrimoine déciderait d'effectuer, afin d'évaluer les risques qu'un traitement fait peser sur les droits et libertés des personnes et d'identifier les mesures à mettre en œuvre pour faire face à ces risques, et la consultation de l'autorité de contrôle.

- afin de permettre à la Cité de l'architecture et du patrimoine de respecter ses obligations au regard de la réglementation Informatique et libertés, telles que notamment ses obligations de notification à l'autorité de contrôle et de communication d'une violation de données aux personnes concernées.

En cas de contrôle d'une autorité compétente, les Parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le Titulaire en tant que responsable du traitement, le Titulaire fera son affaire du contrôle et s'interdira de communiquer ou de faire état des données à caractère personnel de la Cité de l'architecture et du patrimoine.

Dans le cas où le contrôle mené chez le Titulaire concernerait les traitements mis en œuvre au nom et pour le compte de la Cité de l'architecture et du patrimoine, le Titulaire s'engage à en informer immédiatement la Cité de l'architecture et du patrimoine et à ne prendre aucun engagement pour elle.

En cas de contrôle d'une autorité compétente chez la Cité de l'architecture et du patrimoine portant notamment sur les prestations délivrées par le Titulaire, ce dernier s'engage à coopérer avec la Cité de l'architecture et du patrimoine et à lui fournir toute information dont cette dernière pourrait avoir besoin ou qui s'avèrerait nécessaire.

14. Responsabilité

Le titulaire assume la responsabilité de dépositaire. Il est responsable de la conservation et de l'entretien des biens confiés. Il ne peut en disposer qu'aux fins prévues au marché. Il est présumé responsable des avaries et des pertes des objets qui lui ont été confiés. Il ne pourra s'exonérer de cette responsabilité qu'en invoquant la force majeure ou un vice propre de la chose.

En cas de non restitution des biens dans les conditions prévues, la Cité de l'architecture et du patrimoine procédera après avis de l'huissier de justice ou du notaire à une refaction du prix sur la facture correspondante, nonobstant tout recours de garantie contre le titulaire.

Le titulaire assumera seul et entièrement, pendant la durée du contrat, devant la Cité de l'architecture et du patrimoine et tout tiers, l'entière responsabilité liée à l'exécution des prestations pour lesquelles il est engagé.

Pour le titulaire

Le représentant de la Cité de l'architecture et du patrimoine
