

ANNEXE AU CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIÈRES RELATIVE AU TRAITEMENT DES DONNEES PERSONNELLES

La présente annexe ne s'applique que dans l'hypothèse où le titulaire a accès et est amené à traiter des données personnelles (ci-après désignées les « Données ») au sens de l'article 4-1) Définitions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 applicable à compter du 25 mai 2018 (ci-après désigné le « *Règlement* »), pour le compte du pouvoir adjudicateur dans le cadre de l'exécution du présent marché. Dans le cas contraire, les parties reconnaissent expressément que la présente annexe ne leur est pas opposable. A ce titre, les parties déclarent que le titulaire agit en tant que sous-traitant au sens de l'article 4-8) du Règlement. De son côté, le pouvoir adjudicateur agit en tant que responsable de traitement au sens de l'article 4-7) dudit Règlement.

Article 1^{er} - Respect de la réglementation applicable en matière de protection des Données

Chacune des parties s'engage à respecter toutes les obligations résultant de l'application de toute réglementation applicable relative à la protection des Données, en particulier les dispositions issues du Règlement. A cette fin, elles reconnaissent être soumises à une obligation de collaboration renforcée pendant toute la durée du présent marché et s'engagent donc mutuellement à se transmettre sans délai toute information, renseignement, document ou fichier leur permettant de maintenir ou de démontrer leur conformité à la réglementation applicable et à s'informer immédiatement de tout manquement ou risque de manquement à ladite réglementation.

Article 2 - Description du traitement de Données confié au titulaire

Le titulaire est autorisé à traiter pour le compte du pouvoir adjudicateur, pour la durée du présent marché, les Données nécessaires :

- au suivi et à l'administration des prestations, objet du marché ;
- à la facturation et à la comptabilité (sur la base du respect d'obligations légales et réglementaires). Il est entendu que le titulaire à l'interdiction d'utiliser les Données autrement que pour sa mission prévue dans le présent marché. Il a notamment l'interdiction d'utiliser à titre commercial les Données ;

La nature des opérations réalisées sur les Données est : consultation, collecte, enregistrement, stockage provisoire, et traitement des Données.

Les types de Données traitées sont : nom, prénom, qualité, coordonnées professionnelles (notamment adresse électronique et numéros de téléphone fixe et mobile).

Les catégories de personnes concernées sont le personnel du pouvoir adjudicateur et les visiteurs du site de Sèvres – Manufacture et musée nationaux.

Article 3 - Obligations du titulaire vis-à-vis du pouvoir adjudicateur

Le titulaire s'engage à :

- traiter les Données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du présent marché.

- traiter les Données conformément aux instructions documentées du pouvoir adjudicateur. Si le titulaire considère qu'une instruction constitue une violation du Règlement ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des Données, il en informe immédiatement le pouvoir adjudicateur. 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'État 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.

- garantir la confidentialité des Données traitées dans le cadre du présent marché.

- veiller à ce que les personnes autorisées à traiter les Données s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité, d'une part, et reçoivent la formation nécessaire en matière de protection des Données, d'autre part.

- 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.

- aider, dans la mesure du possible, le pouvoir adjudicateur 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). Le titulaire doit répondre, au nom et pour le compte du pouvoir adjudicateur et dans les délais prévus par le Règlement aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des Données faisant l'objet du présent marché.

- notifier au pouvoir adjudicateur toute violation de Données dans un délai maximum de 24 heures après en avoir pris connaissance et par message électronique. Cette notification est accompagnée de toute documentation utile afin de permettre au pouvoir adjudicateur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente ainsi qu'aux personnes concernées.

En parallèle de l'information du pouvoir adjudicateur, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte du pouvoir adjudicateur, les violations de Données dans un délai maximum de **72** heures à compter de la prise de connaissance de la violation de données, 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 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 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 ;
- la description des mesures prises ou que le pouvoir adjudicateur propose de prendre 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.

Après accord écrit du pouvoir adjudicateur, le titulaire communique, au nom et pour le compte du pouvoir adjudicateur, la violation de Données 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 et contient au moins :

- 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 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 ;
- la description des mesures prises ou que le pouvoir adjudicateur propose de prendre pour remédier à la violation de Données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

- aider le pouvoir adjudicateur pour la réalisation d'analyses d'impact relatives à la protection des Données, d'une part, et pour la réalisation de la consultation préalable de l'autorité de contrôle, d'autre part.

- communiquer au pouvoir adjudicateur 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, ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

- mettre à la disposition du pouvoir adjudicateur 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.

- fournir, au moment de la collecte des Données, aux personnes concernées par les opérations de traitement l'information relative aux traitements de Données qu'il réalise. La formulation et le format de l'information doit être convenue avec le pouvoir adjudicateur avant la collecte de Données.

- mettre en œuvre les mesures techniques et organisationnelles permettant de garantir la sécurité, l'intégrité et la confidentialité des Données. Il s'engage notamment à :

- assurer une gestion des Données traitées séparée de la gestion de ses propres Données ou de Données d'autres clients ou fournisseurs,
- ne pas conserver les Données au-delà de la durée de conservation fixée par le responsable de traitement au regard des finalités pour lesquelles elles ont été collectées, et en tout état de cause à ne pas les conserver après la fin de la relation contractuelle,
- protéger les Données en veillant à ce qu'elles ne soient ni déformées, ni endommagées,
- ne rendre accessibles et consultables les Données traitées qu'à ses seuls personnels dûment habilités et autorisés en raison de leurs fonctions et qualité,
- ne pas utiliser ni céder à quelque titre que ce soit les Données personnelles sans l'accord préalable et exprès du pouvoir adjudicateur,
- mettre en place les moyens permettant de rétablir la disponibilité des Données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique,
- le cas échéant, assurer la pseudonymisation et le chiffrement des Données.

- tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du pouvoir adjudicateur comprenant :

- le nom et les coordonnées du pouvoir adjudicateur 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 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, 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,
 - 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 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.

Article 4 – Obligations du pouvoir adjudicateur vis-à-vis du titulaire

Le pouvoir adjudicateur s'engage à :

- fournir au titulaire les données visées à l'article 2 ci-avant ;
- 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 RGPD et par la loi Informatique et Libertés de la part du titulaire ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.

Article 5 - Sort des Données

Au terme du marché, le titulaire s'engage à renvoyer toutes les Données au pouvoir adjudicateur. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire. Une fois détruites, le titulaire doit justifier par écrit de la destruction sur simple du pouvoir adjudicateur dans un délai de quinze (15) jours à compter de la réception de la demande.

Article 6 - Dispositions applicables en cas de sous-traitance

Le pouvoir adjudicateur n'autorise pas une sous-traitance des prestations confiées au titulaire relatives au traitement des Données.