**ANNEXE N°2 A L’AE**

**PROTECTION DES DONNEES PERSONNELLES**

Le Centre des monuments nationaux,

établissement public à caractère administratif domicilié à :

Hôtel de Sully

62, rue Saint-Antoine

75186 Paris Cedex 04,

et représenté par son/sa Président(e)

ci-après *« le responsable de traitement »*

d’une part,

et

Titulaire du marché / co-contractant

[…],

et représenté par […]

ci-après « *le sous-traitant* »

d’autre part,

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s’engagent à prendre toutes les mesures techniques et organisationnelles nécessaires au respect de la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, *« le règlement européen sur la protection des données »*) et la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

II. Description du traitement faisant l’objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour : […]

La nature des opérations réalisées est : […]

Les finalités du traitement sont : […]

Les types de données à caractère personnel traitées sont : […]

Les catégories de personnes concernées sont : […]

III. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données uniquement pour la ou les seules finalités qui font l’objet de la sous-traitance ;
2. traiter les données conformément aux instructions documentées du responsable de traitement. Si le sous-traitant 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 États membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant 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 ;
3. garantir la confidentialité et la sécurité des données à caractère personnel traitées ;
4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

* 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 ;

1. 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.
2. aider le sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations :

* le sous-traitant aide le responsable de traitement **pour la réalisation d’analyses d’impact relative à la protection des données ;**
* le sous-traitant aide le responsable de traitement **pour la réalisation de la consultation préalable de l’autorité de contrôle.**

IV. Sous-traitance ultérieure

**Pas de sous-traitance ultérieure = Option A**

**Option A**

Le sous-traitant n’est pas autorisé à recourir à un autre sous-traitant (ci-après, ***« le sous-traitant ultérieur »***). Si le sous-traitant doit faire appel à un sous-traitant ultérieur pour l’exécution de la prestation de services, il en informe le responsable de traitement. La sous-traitance ultérieure aura lieu dans les conditions décidées par le responsable de traitement (option B ou C).

**Sous-traitance ultérieure = Choisir l’une des deux options**

**Option B (autorisation générale) *Si le sous-traitant ultérieur n’est pas connu***

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, ***« le sous-traitant ultérieur »***) pour mener des activités de traitement spécifiques. 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. Le responsable de traitement dispose d’un délai minium de […] 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.

**Option C (autorisation spécifique) *Si le sous-traitant ultérieur est déjà connu***

Le sous-traitant est autorisé à faire appel à l’entité […] (ci-après, le ***« sous-traitant ultérieur »***) pour mener les activités de traitement suivantes : […]

En cas de recrutement d’autres sous-traitants ultérieurs, le sous-traitant doit recueillir l’autorisation écrite, préalable et spécifique du responsable de traitement.

**Quelle que soit l’option (autorisation générale ou spécifique)**

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s’assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l’exécution par l’autre sous-traitant de ses obligations.

V. 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.

VI. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant 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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à […]. Tout changement d’interlocuteur sera communiqué par courriel.

VII. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement (conjointement à son contact habituel et au délégué à la protection des données) toute violation, ou toute suspicion de violation, de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par le moyen suivant : courrier électronique à […]. Tout changement d’interlocuteur sera communiqué par courriel.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente. Après accord du responsable de traitement, le sous-traitant 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 sous-traitant 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.

VIII. Mesures de protection des données

Le sous-traitant s’engage à mettre en œuvre les mesures de protection et de sécurité prévues par [*code de conduite, certification*].

Le sous-traitant s’engage à mettre en œuvre les mesures de protection et de sécurité suivantes :

VIII.1 Mesures de pseudonymisation, chiffrement et/ou hachage des données à caractère personnel

[…]

VIII.2 Moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement

[…]

VIII.3 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

[…]

VIII.4 Procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement

[…]

IX. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s’engage à respecter les consignes données par le responsable de traitement concernant le sort des données personnelles (par exemple, détruire toutes les données à caractère personnel et transmettre toutes les données à caractère personnel au responsable de traitement).

X. Délégué à la protection des données

Le sous-traitant 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.

XI. Registre des catégories d’activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du responsable de traitement comprenant :

* 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.

XII. Documentation et audits

Le sous-traitant 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.

XIII. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s’engage à :

* documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
* 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 sous-traitant ;
* superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.