##### Institut national de recherches archéologiques préventives - Accueil

##### Accord de sous-traitance relative à la protection des données à caractère personnel (RGPD)

**Assistance, maintenance évolutive, adaptative, corrective et hébergement du logiciel open source Collective Access**

**Entre**

Institut national de recherches archéologiques préventives, dont le siège est situé au 121 rue d’Alésia, 75014 Paris représentée par son Président, Monsieur Dominique Garcia,

Ci-après dénommée l’« INRAP »

D’une part,

**Et**

[à compléter], située à [à compléter] et représentée par [à compléter]

Ci-après dénommé « le titulaire »

D’autre part,

Ci-après désignées collectivement les Parties.

**Il est convenu ce qui suit :**

Pour les besoins du présent accord, les Parties sont dénommées conformément aux définitions énoncées à l’article 4 du règlement (UE) 2016/679 du 27 avril 2016 (ci-après, le « RGPD ») comme suit :

* le titulaire est dénommé le « Sous-traitant » ;
* l’acheteur est dénommé l’« INRAP ».

Le Sous-traitant déclare être en conformité avec la réglementation en vigueur applicable aux traitements de données à caractère personnel et en particulier au RGPD ainsi qu’aux dispositions de la loi du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés.

# Objet

Le présent accord a pour objet de définir les conditions dans lesquelles le Sous-traitant, s’engage à effectuer pour le compte de l’INRAP, en sa qualité de responsable de traitement, des opérations de traitement de données à caractère personnel.

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

Le Sous-traitant est autorisé à effectuer pour le compte de l’INRAP les traitements de données à caractère personnel décrits ci-après :

**L’objet du traitement** est la reprise, la refonte graphique et fonctionnelle et la maintenance du site portail de l’Inrap.

**La nature des opérations réalisées sur les données** sont les suivantes [à confirmer/compléter] :

Collecte de données

Enregistrement de données

Organisation de données

Structuration de données

Conservation de données

Adaptation ou modification de données

Extraction de données

Consultation de données

Utilisation de données

Communication de données (transmission ou toute autre forme de mise à disposition)

Rapprochement de données

Interconnexion de données

Limitation de données

Effacement de données

Destruction de données

**Les finalités du traitement sont :** [à compléter/confirmer]

- la reprise des données du site actuel comprenant le domaine principal ( le portail), plusieurs sous-domaines et rubriques pour réaliser une migration des contenus vers le nouveau site  ;

- la gestion des cookies ;

- l’accompagnement-conseil sur les orientations graphiques, fonctionnelles pour la refonte du site, les évolutions possibles du site ainsi que la formation à son utilisation.

**Les catégories de données à caractère personnel traitées sont**les suivantes **:**

[à confirmer/compléter]

**Données courantes**

Etat civil, identité, données d’identification, images

Données de connexion (logs, adresse IP, etc.)

Vie personnelle (habitudes de vie, situation familiale, diplômes, niveau d’études, etc.)

Vie professionnelle (coordonnées professionnelles, fonctions, etc.)

Informations d’ordre économique et financier (revenus, situation financière, situation fiscale, RIB, etc.)

Données de localisation (déplacements, données GPS, données GSM, etc.)

Autres, préciser : toutes données personnelles qui figurent dans le fonds d’images fixes et animées qui constitue l’iconothèque de l’INRAP (exemple : image des personnes, voix, etc.)

**Données sensibles ou à caractère hautement personnel**

Données relevant de la prétendue origine raciale ou ethnique

Données révélant des opinions politiques

Données révélant des convictions religieuses ou philosophiques

Données révélant l’appartenance syndicale

Données génétiques

Données biométriques aux fins d’identifier de manière unique une personne

Données concernant la santé

Données concernant l’orientation sexuelle ou la vie sexuelle

Données relatives aux condamnations pénales ou aux infractions

Numéro d’identification dans un registre national unique (NIR)

Les **catégories de personnes** concernées sont :

[à confirmer/compléter]

Agents de l’INRAP

Mineurs

Particuliers

Autres, préciser : utilisateurs du site de l’Inrap et toute personne dont les données figurent dans le fonds d’images du site de l’Inrap

Pour l’exécution du présent marché, l’INRAP met à la disposition du Sous-traitant les informations nécessaires pour la réalisation des opérations de traitement.

**Durée du traitement** **:**

La durée du traitement est la durée du présent marché.

Le Sous-traitant s'engage à appliquer les durées de conservation des données selon les instructions de l’INRAP afin de lui permettre de respecter son obligation d’appliquer une durée de conservation n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

# Formalités

Chacune des Parties fait son affaire des formalités lui incombant au titre de la réglementation applicable en matière de protection des données à caractère personnel.

# Obligations du Sous-traitant vis-à-vis de l’INRAP

Le Sous-traitant s’engage à :

* traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance ;
* ne traiter les données que sur instruction documentée de l’INRAP, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le Sous-traitant est soumis. Dans ce cas, le Sous-traitant informe l’INRAP de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
* informer préalablement l’INRAP de tout transfert de données à caractère personnel en dehors de l'Union européenne, lui fournir la preuve de l'utilisation d'outils de transfert adéquats (décisions d'adéquation, clauses contractuelle types pour le transfert des données à caractère personnel ou règles d'entreprise contraignantes), ainsi que, lorsque cela est requis, la documentation prouvant la mise en place de mesures complémentaires techniques, juridiques ou organisationnelles garantissant un niveau de protection adéquat des droits des personnes concernées ;
* informer immédiatement l’INRAP si, selon lui, 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 ;
* garantir la confidentialité, l’intégrité et la disponibilité des données à caractère personnel traitées dans le cadre du présent marché et pouvoir retracer l’accès à ces données ;
* 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 l’information et 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.
* si le traitement implique l’utilisation et/ou le dépôt de cookies et traceurs visés dans les cas prévus à l’article 82 de la Loi Informatique et libertés, le Sous-traitant est tenu :
* d’informer les personnes de manière claire et complète sur les finalités des cookies et traceurs et sur les moyens de s’opposer à leur dépôt ainsi que d’exercer leur droit d’opposition ;
* de recueillir le consentement de la personne concernée lorsque la finalité du cookie ou du traceur le requiert ;
* de prévoir au sein du site impliquant le dépôt de cookies et/ou traceurs, une politique cookies, un module de gestion des cookies ainsi qu’un bandeau cookie conforme aux exigences de la réglementation relative à la protection des données et des recommandations de la Cnil et du CEPD.

Le Sous-traitant s'interdit :

* de divulguer, sous quelque forme que ce soit, tout ou partie des données exploitées ;
* de prendre copie ou de stocker, quelles qu'en soit 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 au cours de l'exécution du marché ;
* d’effectuer pour son compte ou pour le compte de tiers des recherches, analyses, statistiques non prévues par les instructions de l’INRAP, même sous une forme agrégée, pseudonymisée ou anonymisée.

# Mesures techniques et organisationnelles de sécurité du traitement

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le Sous-traitant prend toutes les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté aux risques.

Pour ce faire, le Sous-traitant s’engage à mettre en œuvre les mesures techniques et organisationnelles définies à l’Annexe 1 « Mesures de sécurité ».

Le Sous-traitant s’engage à maintenir ses moyens au cours de l’exécution du présent marché et à défaut, à en informer immédiatement l’INRAP.

# Sous-traitance des prestations du Sous-traitant

Le Sous-traitant n’est pas autorisé à sous-traiter à un sous-traitant ultérieur les opérations de traitement qu’il effectue pour le compte de l’INRAP en vertu du présent marché sans l’autorisation écrite spécifique préalable de l’INRAP. Le Sous-traitant soumet la demande d’autorisation spécifique au moins 21 jours avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre à l’INRAP de prendre une décision au sujet de l’autorisation en ce compris notamment les activités de traitement sous-traitées, l’identité et les coordonnées du sous-traitant, les dates du contrat de sous-traitance, ainsi que tout élément permettant de justifier des garanties de sécurité mises en œuvre par le sous-traitant ultérieur pressenti.

La liste des sous-traitants ultérieurs autorisés par l’INRAP figure à l’annexe 2, que les Parties tiennent à jour.

Les opérations de traitement effectuées par le sous-traitant ultérieur concerné doivent être régies par un contrat ou un autre acte juridique revêtant la forme écrite, y compris la forme électronique.

Le sous-traitant ultérieur est tenu de respecter les obligations prévues à la présente annexe pour le compte et selon les instructions de l’INRAP. Il appartient au Sous-traitant initial de s’assurer que tous les sous-traitants ultérieurs intervenant sur les opérations de traitement effectuées pour le compte de l’INRAP présentent 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 RGPD. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Sous-traitant initial demeure pleinement responsable devant l’INRAP de l’exécution par l’autre sous-traitant de ses obligations.

L’INRAP se réserve, à tout moment pendant la durée du présent marché et notamment lors de la réalisation d’audits, la faculté :

* de demander la communication des contrats conclus entre le Sous-traitant et les sous-traitants ultérieurs afin de vérifier s’ils imposent les mêmes obligations que celles prévues dans la présente annexe.
* de vérifier les garanties présentées par les sous-traitants ultérieurs afin de s’assurer qu’elles sont suffisantes pour garantir la conformité des activités de traitements concernées aux exigences du RGPD et de la Loi Informatique et libertés.

# Exercice des droits des personnes

Le Sous-traitant aide l’INRAP, par tout moyen approprié, à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées.

Dans le cadre de cette assistance, le Sous-traitant tiendra compte des éventuelles restrictions dont les droits des personnes concernées peuvent faire l’objet.

Lorsque les personnes concernées exercent auprès du Sous-traitant des demandes d’exercice de droits, le Sous-traitant doit adresser ces demandes dès réception par courrier électronique à l’adresse suivante : [données-personnelles@inrap.fr](mailto:données-personnelles@inrap.fr).

# Notification des violations de données à caractère personnel

Le Sous-traitant notifie à l’INRAP toute violation de données ou toute suspicion de violation de données à caractère personnel dès qu’il en a pris connaissance et sans retard indu dans un délai maximal de 24h par mail à l’adresse suivante : [données-personnelles@inrap.fr](mailto:données-personnelles@inrap.fr).

Cette notification est accompagnée de toute documentation utile afin de permettre à l’INRAP, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente dans les 72 heures après la prise de connaissance de la violation.

Les informations complémentaires obtenues par le Sous-traitant par la suite seront communiquées de manière échelonnée sans retard indu.

En tout état de cause, en cas de violation, le Sous-traitant s’engage à collaborer avec l’INRAP, à procéder aux investigations permettant, au fur et à mesure de leur réalisation, à l’INRAP de disposer de toute information utile sur l’incident. Le Sous-traitant s’engage en outre à mettre immédiatement en place, à ses frais, les mesures correctrices pour empêcher qu’une telle faille puisse perdurer et/ou se reproduire et réparer les conséquences dommageables.

Lorsque l’INRAP doit gérer une violation de données à caractère personnel qui concerne les traitements réalisés par le Sous-traitant, ce dernier, à la demande de l’INRAP, l’aide à respecter son obligation de communication de la violation aux personnes concernées lorsque la violation est susceptible d’engendrer un risque élevé pour ses droits et libertés.

# Assistance du Sous-traitant

Dans toute la mesure du possible, le Sous-traitant aide l’INRAP pour :

* la réalisation d’analyses d’impact relatives à la protection des données ;
* la réalisation de la consultation préalable de l’autorité de contrôle

# Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le Sous-traitant s’engage à renvoyer toutes les données à caractère personnel à l’INRAP ou au sous-traitant désigné par l’INRAP.

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du Sous-traitant, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel.

Une fois les données détruites, le Sous-traitant doit justifier par écrit de la destruction auprès de l’INRAP.

# Délégué à la protection des données

Le Sous-traitant communique à l’INRAP 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.

# 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 de l’INRAP comprenant :

* le nom et les coordonnées de l’INRAP pour le compte de laquelle 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 de l’INRAP ;
* 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 RGPD, 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.

# Documentation et gestion de la preuve

Le Sous-traitant met à la disposition de l’INRAP toutes les informations nécessaires pour démontrer le respect de toutes ses obligations prévues dans les présentes.

Cette documentation sera notamment constituée de tous les éléments permettant de démontrer que les traitements sont effectués conformément à une instruction de l’INRAP.

# Audit

Le Sous-traitant permettra la réalisation d'audits, y compris des inspections, par l’INRAP ou un autre auditeur mandaté par ce dernier.

Le Sous-traitant s’engage à contribuer à la réalisation de ces audits.

Dans le cas où le Sous-traitant ferait l'objet d'une enquête ou d'une demande d'information par l'autorité de contrôle concernant tout traitement effectué pour le compte de l’INRAP, le Sous-traitant s'engage à en informer l’INRAP, au plus tard dans les 24 heures suivantes à la demande d’information de l’autorité de contrôle et à satisfaire cette enquête ou demande.

# Obligations de l’INRAP vis-à-vis du Sous-traitant

L’INRAP s’engage à :

* fournir au Sous-traitant les données nécessaires à la mise en œuvre de ses obligations ;
* 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 la réglementation applicable en matière de protection des données à caractère personnel de la part du Sous-traitant ;
* superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.

##### ANNEXE 1 : Mesures de sécurité – Liste complète des mesures techniques et organisationnelles

| N° | Mesures techniques et organisationnelles de sécurité mises en œuvre par le sous-traitant |
| --- | --- |
|  | Information et sensibilisation des personnes manipulant les données |
|  | Charte informatique ayant force contraignante |
|  | Identifiant (login) unique pour chaque utilisateur |
|  | Politique de mot de passe utilisateur |
|  | Profils d’habilitation stricts |
|  | Suppression des permissions d’accès obsolètes |
|  | Revue annuelle des habilitations |
|  | Système de journalisation |
|  | Procédures pour les notifications de violation de données à caractère personnel |
|  | Procédure de verrouillage automatique de session |
|  | Antivirus régulièrement mis à jour |
|  | « Pare-feu » (firewall) logiciel |
|  | Sauvegardes ou synchronisations régulières des données |
|  | Limitation des flux réseau au strict nécessaire |
|  | Limitation de l’accès aux outils et interfaces d’administration aux seules personnes habilitées |
|  | Installation sans délai des mises à jour critiques |
|  | Disponibilité des données assurée |
|  | Utilisation du protocole TLS |
|  | Stockage des supports de sauvegarde dans un endroit sûr |
|  | Moyens de sécurité pour le convoyage des sauvegardes |
|  | Tests réguliers de la continuité d'activité |
|  | Mise en œuvre des modalités d’accès spécifiques aux données archivées |
|  | Destruction des archives obsolètes de manière sécurisée |
|  | Enregistrement des interventions de maintenance dans une main courante |
|  | Encadrement des interventions par des tiers |
|  | Effacement des données de tout matériel avant sa mise au rebut |
|  | Alarmes anti-intrusion |
|  | Paramétrages respectueux de la vie privée aux utilisateurs finaux |
|  | Tests sur des données fictives ou anonymisées |
|  | [à spécifier, compléter ou supprimer en fonction des mesures de sécurité mises en œuvre] |

##### ANNEXE 2 : Liste des sous-traitants ultérieurs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N° | SOUS TRAITANT ULTERIEUR | INTERLOCUTEUR | SERVICE SOUS-TRAITE | ADRESSE | GARANTIES DE SECURITE |
|  | [A COMPLETER] | [A COMPLETER] | [A COMPLETER] | [A COMPLETER] | [A COMPLETER] |
|  | [A COMPLETER] | [A COMPLETER] | [A COMPLETER] | [A COMPLETER] | [A COMPLETER] |