Mucem

**Département des systèmes d’information**

**CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIERES (CCAP)**

**Annexe 2 : Traitement de données à caractère personnel pour le compte du Mucem**

**OBJET DU CONTRAT IMPLIQUANT LE TRAITEMENT DE DONNEES :**

**Prestations d’infogérance informatiques pour le Mucem**

# Préambule – précisions terminologiques

Cf. <https://www.cnil.fr/fr/glossaire>

Pour l’application de la présente annexe, le responsable de traitement au sens du RGPD est le Mucem et le sous-traitant est le titulaire du marché public.

La présente clause a pour objet de définir les conditions dans lesquelles le titulaire s’engage à effectuer pour le compte du Mucem les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre du présent marché public, les parties s’engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment le 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, et abrogeant la directive 95/46/CE (ci-après, «règlement général sur la protection des données » RGPD) et la loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés.

# description du traitement de données à caractère personnel

Le titulaire est autorisé à traiter pour le compte du Mucem, pour la durée du présent contrat, les données à caractère personnel nécessaires pour fournir la(les) prestation(s) suivante(s) : Prestations d’infogérance informatiques

La nature des opérations réalisées sur les données est : la consultation des genres, des noms, prénoms et service d’affectation des utilisateurs.

La ou les finalité(s) du traitement sont : la communication et le suivi des incidents avec le demandeur.

Les données à caractère personnel traitées sont : Le Prénom, le Nom

Les catégories de personnes concernées sont : Tous les agents du Mucem

Pour l’exécution des prestations objets du présent contrat, le Mucem met à la disposition du titulaire les informations nécessaires suivantes :

* Le Prénom
* Le Nom
* Le Genre

# Obligations du titulaire vis-à-vis du Mucem (article 28.3 du RGPD)

Le titulaire s’engage notamment à :

* traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet du présent contrat
* traiter les données conformément aux instructions documentées du Mucem. Si le titulaire considère qu’une instruction constitue une violation du règlement général 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 Mucem
* Si le titulaire est tenu de procéder à un transfert de données vers un pays tiers (hors de l’Union européenne) 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 Mucem de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information
* garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat
* 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
* 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.

# Sous-traitance des activités de traitement (articles 28.2 et 28.4 du RGPD)

Lorsque le titulaire fait appel à un sous-traitant pour mener des activités de traitement spécifiques, il informe préalablement et par écrit le Mucem 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.

Afin d'obtenir l'acceptation et l'agrément du Mucem, le titulaire doit présenter son sous-traitant par le biais de l'acte spécial de sous-traitance, dont les formalités sont comprises dans le formulaire DC4 ou équivalent (téléchargeable sur <http://www.economie.gouv.fr/daj/formulaires-declaration-candidat>).

Le sous-traitant est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du Mucem. Il appartient au titulaire de s’assurer que le sous-traitant 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 général sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant le Mucem de l’exécution par le sous-traitant de ses obligations.

# Droit d’information et exercice des personnes concernées par le traitement (articles 13 à 15 du RGPD)

Le titulaire doit fournir aux personnes concernées par les opérations de traitement ou de collecte l’information relative aux traitements de données qu’il réalise pour le compte du Mucem, sauf dans le cas où ce dernier procéderait ou aurait procédé lui-même à cette information. Dans ce cas, le Mucem en informe expressément le prestataire.

Le cas échéant, la formulation et le format de l’information doivent être convenus avec le responsable de traitement avant la collecte de données.

Les personnes disposent d’un droit d’accès, de rectification, d’effacement et d’opposition des données les concernant. Elles disposent également d’un droit à la portabilité des données transmises au responsable de traitement. Ce droit s’applique dans les mêmes conditions que le droit d’accès et de rectification.

Lorsque les personnes concernées exercent auprès du titulaire des demandes d’exercice de leurs droits, le titulaire doit adresser ces demandes dès réception par courrier électronique au délégué à la protection des données du Mucem à l’adresse [dpo@mucem.org](mailto:dpo@mucem.org).

# Notification des violations de données à caractère personnel (article 33 du RGPD)

Le titulaire notifie au Mucem toute violation de données à caractère personnel dans un délai de **24** heures après en avoir pris connaissance et par courriel adressé à l’interlocuteur en charge du marché et en copie à l’adresse suivante : dpo@mucem.org.

Cette notification est accompagnée de toute documentation utile afin de permettre la notification par le titulaire de cette violation à l’autorité de contrôle compétente (en l’occurrence, à la Commission nationale de l’informatique et des libertés, CNIL) si possible 72 heures au plus tard après en avoir pris connaissance.

En parallèle de l’information du Mucem, le titulaire notifie à l’autorité de contrôle compétente, au nom et pour le compte du Mucem, les violations de données à caractère personnel 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 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 l’acheteur 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 écrit du Mucem, le titulaire communique, au nom et pour le compte du Mucem, 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 l’acheteur 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.

# Aide du titulaire dans le cadre du respect par le Mucem de ses obligations

Le titulaire aide l’acheteur :

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

# Mesures de sécurité

Le prestataire s’engage à 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 personnelles 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 du Mucem.
* mettre en place 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 cas échéant, assurer la pseudonymisation et le chiffrement des données à caractère personnel

# Sort des données (article 28.3.g du RGPD)

Au terme de l’exécution du présent contrat, le titulaire doit détruire toutes les données à caractère personnel.

Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

# Délégué à la protection des données (articles 37 à 39 du RGPD)

Le titulaire communique au Mucem **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, ou, à défaut, l’identité et les coordonnées d’un point de contact dédié à ces questions.

# Registre des activités de traitement (article 30 du RGPD)

Le titulaire tient par écrit un registre de toutes les activités de traitement effectuées pour le compte du Mucem comprenant :

* le nom et les coordonnées du Mucem, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données
* les catégories de traitements effectués pour le compte du Mucem
* 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 général 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, notamment, 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 (article 28.3.h du RGPD)

Le titulaire met à la disposition du Mucem la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre, le cas échéant, la réalisation d'audits, y compris des inspections, par le Mucem ou un auditeur mandaté par lui, et contribuer à ces audits.

# obligations du Mucem vis-à-vis du titulaire

Le Mucem s’engage à :

* Documenter par écrit toute instruction concernant le traitement des données par le titulaire
* Veiller 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, le cas échéant, réaliser des audits et des inspections auprès du titulaire

# Signature du titulaire

A ………..

Le

Signature :