PRÉFET
DE LA RÉGION
AUVERGNE-
RHÔNE-ALPES
*Liberté*
*Égalité*
*Fraternité*

**Secrétariat général**
**pour les affaires régionales**

**Accord-cadre régional interministériel relatif aux prestations de maintenance et de petits travaux d'entretien des couvertures et des étanchéités sur les sites du patrimoine de l'État et de certains établissements publics de la région Auvergne-Rhône-Alpes**

**ANNEXE 3 AU CCAP**

**TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL**
**MESURES DE SÉCURITÉ**

n° de référence de l'accord-cadre : COUV_ETANCH_ARA_2027

La présente annexe comporte 8 pages.

# TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

**1. Cas de l'acheteur**

Le présent article a pour objet de définir les conditions dans lesquelles le titulaire du présent accord-cadre s'engage à effectuer pour le compte de l'acheteur les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre du présent accord-cadre, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment le RGPD et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

**- Précisions terminologiques**
Le responsable de traitement au sens 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, et abrogeant la directive 95/46/CE (ci-après, «règlement général sur la protection des données » ou RGPD) est l'acheteur et le sous-traitant est le titulaire du présent accord-cadre.

**- Nature, durée, finalité et description du traitement de données à caractère personnel**
Le titulaire est autorisé à traiter pour le compte de l'acheteur, les données à caractère personnel nécessaires pour fournir les prestations objet de l'accord-cadre.
Les données à caractère personnel sont traitées pour une durée identique à celle de l'accord-cadre.

**- Obligations du titulaire vis-à-vis de l'acheteur**
Le titulaire de l'accord-cadre s'engage, notamment, à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du présent accord-cadre ;

2. 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'État membre auquel il est soumis, il doit informer l'acheteur de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information ;

Les données transférées vers un pays tiers doivent bénéficier d'un degré de protection équivalent à celui garanti par le RGPD au sein de l'Union européenne. Il est rappelé que tout transfert de données à caractère personnel, au bénéfice de toute entité et notamment de pays tiers ou d'organisations internationales, qui ne serait pas strictement conforme à la réglementation française ou européenne est formellement prohibé.

À défaut de pouvoir garantir le respect de ces exigences en cas de transfert de données à caractère personnel vers un pays tiers, le titulaire suspend tout transfert et se rapproche de l'acheteur pour envisager, le cas échéant, l'adaptation des modalités d'exécution de l'accord-cadre permettant le respect des exigences du RGPD.

Si les modalités d'exécution ne peuvent être adaptées, l'acheteur procède à la résiliation de l'accord-cadre pour motif d'intérêt général dans les conditions prévues par le CCAG de référence.

3. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent accord-cadre ;

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent accord-cadre :

- 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

5. 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**

Lorsque le titulaire fait appel à un sous-traitant pour mener des activités de traitement spécifiques, il informe préalablement et par écrit l'acheteur. Cette information doit indiquer clairement la nature des activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Cette sous-traitance ne peut être effectuée que si l'acheteur n'a pas émis d'objection pendant le délai de 21 jours à compter de la date de réception de la demande en application des dispositions de l'article R.2193-4 du Code de la commande publique.

Afin d'obtenir l'acceptation et l'agrément de l'acheteur, le titulaire doit présenter son sous-traitant conformément aux modalités définies à l'article 15 du CCAP.

Le sous-traitant est tenu de respecter les obligations du présent accord-cadre pour le compte et selon les instructions de l'acheteur. 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 de la législation et de la réglementation en vigueur 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 l'acheteur de l'exécution par le sous-traitant de ses obligations. Le titulaire informe préalablement et par écrit l'acheteur de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants

**- Droit d'information et exercice des personnes concernées par le traitement**

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

La formulation et le format de l'information doivent être convenus avec l'acheteur avant la collecte de données.

Le titulaire doit répondre, au nom et pour le compte de l'acheteur et dans les délais prévus par le règlement général sur la protection des données, aux demandes des personnes concernées en cas d'exercice de leurs droits.

**- Notification des violations de données à caractère personnel**

Le titulaire notifie à l'acheteur toute violation de données à caractère personnel dans un délai de 24 heures après en avoir pris connaissance et par courriel. Cette notification est accompagnée de toute documentation utile afin de permettre à l'acheteur, si nécessaire, de notifier 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.

Après accord écrit de l'acheteur, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte de l'acheteur, les violations de données à caractère personnel dans un délai maximum de 72 heures 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 de l'acheteur, le titulaire communique, au nom et pour le compte de l'acheteur, 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 l'acheteur de ses obligations :**

Le titulaire aide l'acheteur :

- à la réalisation d'analyses d'impact relatives à la protection des données ;
- à la réalisation de la consultation préalable de l'autorité de contrôle.

Le titulaire met à la disposition de l'acheteur 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 l'acheteur ou un auditeur mandaté par lui, et contribuer à ces audits.

**- Mesures de sécurité**
Le titulaire met en œuvre les mesures de sécurité suivantes :

- 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 ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

**- Sort des données**
Au terme de l'exécution du présent accord-cadre, l'acheteur informe le titulaire de sa décision relative au sort des données. L'acheteur peut demander au titulaire de :

- détruire toutes les données à caractère personnel ;
- renvoyer toutes les données à caractère personnel à l'acheteur ou au tiers désigné par l'acheteur.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

**2. Cas des bénéficiaires de l'accord-cadre**

**- Sort des données**
Au terme de l'exécution du présent marché public, le bénéficiaire informe le titulaire de sa décision relative au sort des données. Le bénéficiaire peut demander au titulaire de :

- détruire toutes les données à caractère personnel ;
- renvoyer toutes les données à caractère personnel à l'acheteur ou au tiers désigné par le bénéficiaire.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

**- Délégué à la protection des données**
Le titulaire communique au bénéficiaire dès la notification de l'accord-cadre le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un, ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

**- Registre des activités de traitement**
Le titulaire tient par écrit un registre de toutes les activités de traitement effectuées pour le compte du bénéficiaire comprenant :
1. le nom et les coordonnées de l'acheteur pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
2. les catégories de traitements effectués pour le compte de l'acheteur ;
3. 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 ;

4. 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.

**3. Dans le cadre de la réalisation des engagements insertion**

Le titulaire et ses éventuels co-traitants et/ou sous-traitants traiteront des données à caractère personnel et les transmettront à l'AMO insertion, afin qu'il vérifie l'éligibilité des candidats au dispositif et réalise le suivi des heures d'insertion.

Ils s'engagent à traiter ces données dans le respect du RGPD et des clauses contractuelles conformément à l'article Erreur : source de la référence non trouvée du présent CCAP.

Dans le cas de l'embauche directe, le titulaire informera les candidats et salariés de la transmission à l'AMO insertion des données suivantes : données nécessaires à la vérification de leur éligibilité au dispositif, données nécessaires au suivi des heures d'insertion.
Dans le cas du recours à une structure mettant à disposition du personnel ou à un sous-traitant, le titulaire pourra reporter cette obligation d'information sur la structure en contact direct avec le candidat / salarié, afin de favoriser la bonne compréhension de cette information.

Conformément à la réglementation en vigueur applicable au traitement de données à caractère personnel dans le cadre du RGPD, la Maison Métropolitaine d'Insertion pour l'Emploi (MMI'e) s'engage vis-à-vis des entreprises, dans le cadre de l'exécution de ses prestations, à respecter et à faire respecter par son personnel, les obligations suivantes :

- Ne collecter et traiter les données personnelles que conformément aux instructions et aux finalités liées à l'objet des prestations qui lie les différentes parties,
- Mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir la sécurité, l'intégrité et la confidentialité des données personnelles collectées et d'empêcher qu'elles ne soient déformées, endommagées, perdues, détournées, corrompues, divulguées, transmises ou communiquées à des personnes non autorisées,
- Garantir l'exercice de droit d'accès aux données sur demande (droit d'accès, de rectification, d'effacement et d'opposition), sur simple demande au délégué à la protection des données de la MMI'e (dpd@lyonmetropole-mmie.fr)
- Supprimer ou anonymiser les données personnelles collectées dans un délai maximum de 10 ans.

# MESURES DE SÉCURITÉ

**1. Levées d'inaccessibilité**

Dans le cadre des missions qui lui sont confiées, le titulaire du présent accord-cadre peut être sollicité, sur demande du service bénéficiaire, pour effectuer une visite des locaux identifiés par le responsable de site.

Le cas échéant, il doit s'organiser pour visiter les locaux sensibles et/ou techniques en fonction des disponibilités des occupants/personnes pouvant donner accès aux locaux, en lien avec le service bénéficiaire ou l'accompagnateur désigné par celui-ci, comme indiqué par l'arrêté du 12 décembre 2012 relatif aux critères d'évaluation de l'état de conservation des matériaux et produits de la liste A contenant de l'amiante et au contenu du rapport de repérage et à l'arrêté du 26 juin 2013 relatif au repérage des matériaux et produits de la liste C contenant de l'amiante et au contenu du rapport de repérage.

Si le titulaire n'est pas mis en mesure par le ou les service(s) bénéficiaire(s) concerné(s) d'accéder à un local fermé malgré ses demandes orales et écrites durant la période d'intervention prévue, il pourra demander à réaliser une visite complémentaire selon les modalités de tarification définis dans le bordereau des prix unitaires.

Cette visite complémentaire doit être programmée avec les agents disposant des accès à l'ensemble des locaux potentiellement fermés lors de la première période d'intervention.

Dans le cadre de ce rapport, aucune mention « non inspectée par défaut d'accessibilité » n'est acceptée.

**2. Accès restreint à des zones ou à des sites**

Toute personne relevant du titulaire ou de ses sous-traitants est soumise, le cas échéant, à des mesures de sécurité qu'il s'agisse d'accès physiques à des locaux ou d'accès logiques à des informations.

Le titulaire doit fournir au responsable de chaque site, 48 heures avant tout commencement d'exécution du bon de commande, une liste comportant le nom et le prénom des agents assurant la prestation. Il doit fournir, en outre, lors du démarrage de la prestation et à l'occasion de toute affectation d'un nouvel agent, les renseignements et informations nécessaires à l'établissement des laissez-passer (badges) du présent CCAP, lorsqu'ils sont exigés pour la circulation de ces agents dans les locaux de l'administration.

Le titulaire doit se conformer aux exigences de certains sites dits sensibles notamment quant à la communication du casier judiciaire. Dans ces cas, le service bénéficiaire communiquera par écrit au titulaire les exigences particulières auxquelles le titulaire devra se conformer.

Ces éléments, ou toute autre précision que juge nécessaire le service bénéficiaire, seront annexés au bon de commande.

Le titulaire doit informer le responsable de site de toute évolution dans les effectifs affectés à la prestation.

L'annexe 1 au CCAP précise les conditions d'accès dans les services du ministère de l'Intérieur (police, Gendarmerie), de la direction générale des douanes et des droits indirects et du ministère de la Justice (administration pénitentiaire, justice judiciaire et protection de la jeunesse).

Les prescriptions ci-dessous valent pour tout site dont les accès sont restreints ou dont certaines zones sont réglementées soit par la loi soit par le règlement particulier du site. Le titulaire doit en conséquence se conformer aux stipulations de l'article 5 du CCAG-FCS.

**Contrôle nominatif**

Une liste nominative des personnels intervenant dans les locaux est établie et fournie par le titulaire au service bénéficiaire. Le titulaire doit certifier que tous les personnels qu'il emploie pour l'exécution de la prestation sont en règle vis-à-vis des dispositions légales et réglementaires relatives aux conditions d'emploi de la main-d'œuvre.

**Contrôle des accès**

Tous les personnels des entreprises devront être munis d'un laissez-passer comportant une photographie et les renseignements figurant sur la carte d'identité ou le titre de travail pour les ouvriers étrangers. Des contrôles inopinés de corrélation avec le registre unique du personnel pourront être opérés à tout moment par l'inspection du travail.

La liste des véhicules privés susceptibles de pénétrer dans l'enceinte d'un site est fournie aux services bénéficiaires concernés par le titulaire, dès la notification du présent accord-cadre.

**Restriction de circulation**

Au cas où les nécessités de la sécurité des activités du service bénéficiaire l'exigeraient, ce dernier peut se réserver le droit de refuser à un ou plusieurs agents de l'intervenant l'accès de certains locaux.

Le titulaire doit faire son affaire des zones d'accès restreintes mises en place au sein des services et des établissements. Il doit également faire son affaire des contacts à prendre avec d'éventuels intervenants extérieurs.