Pouvoir adjudicateur

Caisse d'allocations familiales du Val-de-Marne

2 Voie Félix Eboué
94 000 Créteil
Organisme de droit privé chargé d'une mission de service public

Marché n°26-15

Réservation de places en crèches pour les enfants du personnel de la caisse d'allocations familiales du Val-de-Marne

Marché à procédure adaptée passée en application des articles L.2123-1 et R. 2123-1 et suivants du code de la commande publique.

Accord-cadre mono-attributaire à prix unitaires.

SECURITE DES INFORMATIONS ET INFORMATIQUE ET LIBERTES

Article 1 - Obligation de résultat

Le titulaire s'engage à exécuter les obligations, découlant du présent marché avec tout le soin en usage dans sa profession conformément aux normes du moment.
Il est soumis à une obligation de résultat en permanence en raison de la mission de service public de l'organisme contractant. Il s'engage à mettre en œuvre tous les moyens nécessaires à la bonne exécution des prestations qui lui sont confiées.
Il s'engage à assurer une mission d'information, de conseil et d'assistance auprès de l'organisme contractant sur l'exécution des travaux en question.

Article 2 - Obligation de confidentialité et rgpd

Les prestations s'effectuant dans des locaux relevant d'un service public devront conduire le titulaire, s'il avait connaissance de faits ou de circonstances faisant craindre des indiscrétions, à aviser immédiatement l'organisme contractant, en lui fournissant toutes indications pour lui permettre d'éviter ou, en cas de survenance, de limiter et de réparer les risques d'indiscrétion susceptibles de se produire.
Le titulaire et son personnel se reconnaissent soumis au secret professionnel et à l'obligation de discrétion pour tout ce qui concerne les faits, informations, et décisions dont ils auront connaissance au cours de l'exécution du présent marché (articles 226-13 et suivants du code pénal et article 29 de la loi n° 78-17 du 6 Janvier 1978 modifiée par la loi n°2004-801 du 6 août 2004).
L'organisme contractant n'a pas à signaler le caractère confidentiel des faits, informations, décisions pour que cette obligation soit respectée.
Ils s'interdisent notamment toutes communications écrites ou verbales sur ces sujets, ainsi que toute remise de documents et informations à des tiers, personnes morales ou non (privées ou publiques), sans l'accord de l'organisme contractant.
Par ailleurs, les informations obtenues par le titulaire au cours de l'exécution du marché ne peuvent faire l'objet d'aucune divulgation à des tiers ou à des membres de son personnel non appelés à participer à l'exécution des prestations, sauf si la divulgation est nécessaire en raison d'obligations légales, comptables ou réglementaires, échappant au contrôle du titulaire.
Le titulaire s'engage notamment à :

- Ne pas utiliser les informations, données et documents à des fins autres que celles spécifiées par le présent marché ;
- Ne prendre aucune copie des documents et fichiers informatiques qui lui sont confiés ;
- Prendre toutes mesures permettant d'éviter leur utilisation détournée ou frauduleuse
- Ne pas les communiquer à des personnes physiques ou morales, privées ou publiques, autres que celles qui ont qualité pour en connaître, à savoir l'organisme, ainsi que le personnel chargé par le Titulaire d'exécuter les prestations ;
- Ne conserver aucune de ces informations, données et documents, ni aucune copie de ceux-ci, sous quelque forme que ce soit ;
- Alerter immédiatement l'organisme de tout fait faisant craindre que les obligations souscrites au titre du présent article ne seraient pas respectées.

Le titulaire s'engage également à faire respecter les dispositions du présent article par son personnel et par toute personne qui interviendrait directement ou indirectement pour son compte, notamment ses éventuels sous-traitants.
Par ailleurs, il conclut avec ses derniers un engagement de sécurité et de confidentialité reprenant les obligations prévues au présent article, afin d'assurer notamment la mise en

œuvre des mesures de sécurité et de confidentialité conformément à l'article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
L'organisme contractant se réserve le droit de procéder à toute vérification qui lui paraît utile pour s'assurer du respect de ses obligations, tant par le titulaire que par ses sous-traitants éventuels. Pour ce faire, l'organisme se réserve le droit de demander, à tout moment, au titulaire, communication de l'engagement de sécurité et de confidentialité prévu au précédent alinéa.
En cas de violation des obligations susmentionnées, et indépendamment des sanctions pénales éventuellement encourues, le marché peut être résilié aux torts exclusifs du titulaire comme il est prévu au c.c.a.p du présent marché.
La responsabilité du titulaire peut également être engagée sur le fondement des articles 226-17 et 226-5 du code pénal.
Le titulaire respecte les obligations souscrites au titre du présent article pendant la durée de validité du marché puis après sa fin, quelle qu'en soit la cause.

Article 3 - Protection des données à caractère personnel – rgpd

L'attention du titulaire est attirée sur la nécessité de faire respecter un impératif de discrétion absolue quant aux informations que son personnel aurait à connaître à l'occasion de l'exécution des prestations.
Le titulaire du marché s'engage à observer cette obligation. Lors des entretiens avec les allocataires, le personnel est tenu de maintenir confidentiel tout renseignement ou documents quelconques. Les renseignements ou documents ne peuvent, sans autorisation, être communiqués à d'autres personnes que celles qui ont qualité pour en connaître.
Tout renseignement, de quelque nature que ce soit, concernant les activités, l'organisation ou toute autre information relative à l'organisme dont le titulaire pourrait avoir connaissance ou qui lui aurait été communiqué lors de l'exécution du marché, est de nature confidentielle et ne peut être divulgué.
Le titulaire doit prendre toutes les mesures nécessaires pour respecter cette clause et la faire respecter par son personnel. En cas de non-respect de cette clause, le titulaire s'expose à des poursuites pénales.
Le titulaire respecte les obligations souscrites au titre du présent article pendant la durée de validité du marché puis après sa fin, quelle qu'en soit la cause.

Article 4 - Protection des données à caractère personnel

Le sous-traitant (le titulaire) est autorisé à traiter pour le compte du responsable du traitement (l'organisme contractant), les données à caractère personnel nécessaires pour fournir le ou les services/prestations nécessaires à l'exécution du marché.
Dans le cadre des prestations qui lui sont confiées, le sous-traitant peut être amené à traiter des données personnelles concernant les allocataires ou les salariés de la caf du Val-de-Marne, figurant au sein de traitements mis en œuvre par le responsable de traitement, ou peut être amené à y accéder.
Pour l'exécution de sa mission, le responsable de traitement met à la disposition du sous-traitant les données à caractère personnel nécessaires pour l'exécution de ces prestations.

Article 5 - Obligations de l'organisme contractant (ou responsable du traitement)

Le responsable du traitement s'engage à :
a) Respecter les obligations qui lui incombent en sa qualité de responsable de traitement, en vertu des dispositions du rgpd et de la loi Informatique et Libertés ;

b) Fournir au sous-traitant la description du ou des prestations confiées dans le cadre de la présente prestation/marché et documenter par écrit toute instruction concernant le traitement des données ;
c) Mettre à disposition du sous-traitant toutes les données nécessaires à l'exécution de sa mission ; d) Le cas échéant, effectuer une analyse d'impact relative à la protection des données, avec le concours du sous-traitant ;
e) Veiller, au préalable et pendant toute la durée du de la prestation/marché, au respect des obligations prévues par le rgpd de la part du sous-traitant ;
f) Superviser le traitement, y compris par la réalisation d'audits et d'inspections auprès du sous-traitant ;
g) Notifier, le cas échéant, les violations de données à caractère personnel à la commission nationale de l'informatique et des libertés et communiquer, si nécessaire, aux personnes concernées, avec l'assistance du sous-traitant, dans les conditions décrites à l'article 4.3 du présent document.

Article 6 - Obligations du titulaire

Le sous-traitant (ou titulaire du marché) s'engage à :
a) Respecter les obligations qui lui incombent en sa qualité de sous-traitant, en vertu des dispositions du rgpd et de la loi Informatique et Libertés, dont la tenue d'un registre sous-traitant au titre de l'article 30 du rgpd.
b) Traiter les données à caractère personnel uniquement pour la ou les seules finalités faisant l'objet de la sous-traitance et en aucun pour ses propres besoins ou pour les besoins d'un tiers.
c) Traiter les données à caractère personnel conformément aux instructions documentées du responsable du traitement. Si le sous-traitant considère qu'une instruction constitue une violation du rgpd, de la loi n°78-17 du 6 janvier 1978 modifiée ou de toute autre disposition du droit de l'Union européenne ou du droit des Etats membres relatives à la protection des données, il en informe immédiatement le responsable du traitement.
d) Assurer la sécurité et la confidentialité des données à caractère personnel traitées dans le cadre de la présente prestation/ du présent marché, dans les conditions décrites à l'article 8.3.3 du présent document.
e) Respecter son obligation de conseil et signaler au responsable de traitement les mesures de sécurité additionnelles qu'il conviendrait de prendre.
f) Ne pas chercher à lever le pseudonymat de données pseudonymes qui lui auraient été confiées par le responsable de traitement. Informer sans délai le responsable de traitement en cas de réidentification à partir de données insuffisamment anonymisées par le responsable de traitement.
g) Informer le responsable de traitement de toute réquisition ou demande de communication des données personnelles confiées, par un tiers autorisé, sauf si un texte légal l'interdit.
h) Mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du rgpd et dans la présente annexe ;
i) Fournir au responsable de traitement le nom et les coordonnées de son délégué à la protection des données ou de toute autre personne faisant office de délégué à la protection des données pour son compte.

Article 7 - Obligations en cas de sous-traitance

De manière générale, tout sous-traitant ultérieur est tenu de respecter les obligations de la présente annexe et notamment les instructions du responsable de traitement. Il appartient au sous-traitant de s'assurer que le sous-traitant ultérieur qu'il choisit 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 rgpd.
Si le sous-traitant ultérieur ne remplit pas les obligations en matière de protection des données, le sous-traitant demeure pleinement responsable de l'exécution par l'autre sous-traitant de ses obligations.

Article 8 - Transfert de données personnelles vers des pays tiers

Le sous-traitant s'engage à ne rendre accessible ou à ne transférer aucune donnée du responsable de traitement, même à des fins d'acheminement, à toute entité ou tout sous-traitant établi(e) dans un pays situé en dehors de l'union européenne ou assurant un niveau de protection adéquat, sauf avec le consentement préalable et écrit du responsable de traitement.
Le sous-traitant fournira au responsable de traitement l'outil de transfert utilisé pour permettre le flux transfrontières (bcr approuvées, clauses contractuelles types, etc.).

Article 9 - Droits des personnes concernées

Dans la mesure du possible, le titulaire aide le responsable de traitement, sans frais, par des mesures techniques et organisationnelles appropriées, à donner suite aux demandes des personnes concernées en vue d'exercer leurs droits prévus au chapitre III du rgpd. À ce titre, il répond dans les meilleurs délais à toute sollicitation du responsable de traitement.

Article 10 - Information des personnes concernées

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

Article 11 - Exercice des droits des personnes

Lorsque les personnes concernées exercent à tort auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit immédiatement adresser au responsable de traitement et de façon sécurisée ces demandes dès réception, aux coordonnées indiquées par le responsable de traitement afin que ce dernier puisse traiter la demande dans les temps impartis.

Article 12 - Assistance apportée au responsable de traitement

Le titulaire aide le responsable de traitement à démontrer que celui-ci respecte ses obligations légales et réglementaires relatives à la protection des données.

Article 13 - Analyses d'impact relatives à la protection des données

Le titulaire assiste notamment le responsable de traitement pour la réalisation des analyses d'impact relatives à la protection des données prévues à l'article 35 du rgpd et, si besoin, de la consultation préalable de l'autorité de contrôle prévues à l'article 36 du rgpd.

Article 14 - Traitement des incidents de sécurité

Le titulaire aide également le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du rgpd.
À ce titre, il met en place, et il obtient de chacun de ses propres sous-traitants qu'ils mettent en place, pendant toute la durée du marché, un processus de gestion des incidents de sécurité.
Le titulaire notifie au responsable de traitement tout incident de sécurité impactant les données qu'il traite dans le cadre de la prestation qui lui a été confiée. Cette notification intervient dans les plus brefs délais et, en tout état de cause, dans un délai maximum de 48 heures ouvrables après en avoir eu connaissance, aux coordonnées indiquées par le responsable de traitement.
Cette notification est accompagnée de toute information utile pour permettre au responsable de traitement de qualifier l'incident de violation de données au sens de l'article 4.12 du rgpd et, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente au titre de l'article 33 du rgpd, voire de la communiquer aux personnes concernées au titre de l'article 34 du rgpd.
Cette notification contient au moins les informations suivantes :

- La description de l'incident de sécurité : nature, portée, catégories et nombre approximatif d'enregistrements de données personnelles concernées, catégories et nombre approximatif de personnes concernées, temporalité, conséquences.
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel les informations supplémentaires peuvent être obtenues.
- La description des mesures prises, engagés, envisagées ou proposées pour remédier à l'incident de sécurité, y compris, le cas échéant les mesures pour atténuer les éventuels effets négatifs pour les personnes concernées.

S'il n'est pas possible de fournir toutes ces informations en même temps, le sous-traitant peut les communiquer de manière échelonnée, sans délai injustifié. Il en informe le responsable de traitement en lui indiquant des raisons pour lesquelles la totalité des informations ne peuvent être communiquées dans ce délai.
Le sous-traitant s'engage à coopérer pleinement, à ses frais, avec le responsable de traitement afin de l'aider dans la gestion de cette situation et notamment en :

- L'aidant à la conduite des investigations sur l'incident de sécurité.
- Fournissant au responsable de traitement ou au tiers indépendant qu'il a désigné, un accès physique aux installation et opérations concernées .
- Organisant des entretiens entre le personnel du responsable de traitement et son propre personnel.
- Fournissant tous les registres, journaux, dossiers, communications de données et autres documents pertinents nécessaires pour se conformer à la réglementation en vigueur et, le cas échéant, aux codes de conduite auxquels il aurait adhéré.

Le titulaire s'engage à ne pas informer les tiers, y compris les personnes concernées mais à l'exception des autorités de contrôle, de tout incident de sécurité ou de toute violation de données traitées dans le cadre de la présente prestation/présent marché, sans avoir obtenu le consentement préalable et écrit du responsable de traitement.
Le titulaire reconnaît que le responsable de traitement est seul habilité à :

- déterminer si l'incident de sécurité constitue ou non une violation de données à caractère personnel ;
- décider cette violation doit ou non être notifiée à l'autorité de contrôle, voire communiquée aux personnes concernées ;
- formaliser le contenu de ladite notification ;
- réaliser la notification proprement dite à la cnil.

Lorsque le responsable de traitement est dans l'obligation de communiquer la violation de données à caractère personnel aux personnes concernées, le sous-traitant prend en charge les frais liés à cette communication si la violation est survenue à cause d'un manquement du sous-traitant aux obligations prévues par la présente et au rgpd.
A la suite à une éventuelle violation de données, le sous-traitant assiste le responsable de traitement pour répondre à toute enquête ou demande émanant d'une autorité de

contrôle, voire à toute plainte formulée par une personne concernée ou par un regroupement de celles-ci.
En cas de manquement du sous-traitant au titre de ses obligations décrites dans la présente annexe, celui-ci restaure, à ses frais, les données traitées dans le cadre du présent marché en cas de perte de données.
Le sous-traitant tient et met à disposition du responsable de traitement un registre des incidents de sécurité qui ont impacté les données confiées et y documente, au minimum, toute information pertinente concernant les circonstances de ces incidents de sécurité, ses effets et les mesures prises à ses frais pour y remédier et éviter qu'ils ne se reproduisent.

Article 15 - Sécurité des données

Le titulaire reconnait que la sécurité est un critère fondamental pour la protection des données à caractère personnel et s'engage à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au niveau de risque déterminé par le responsable de traitement.
Celles-ci tiennent compte de l'état de l'art, de la doctrine de la cnil et de l'anssi et sont conformes aux standards de sécurité en vigueur. Elles ne doivent en aucun cas être moins rigoureuses que celles mises en place par le sous-traitant pour le traitement de ses propres données.
Le sous-traitant s'engage à communiquer au responsable de traitement, sur simple demande, tout document décrivant sa politique de sécurité des informations, les mesures de sécurité mises en œuvre, les certifications obtenues et les résultats synthétiques des audits de sécurité qu'il fait réaliser. Ces documents sont considérés comme confidentiels.

Article 16 - Engagements de sécurité

Le titulaire s'engage expressément à :
a) Prendre en compte les principes de protection des données par défaut et dès la conception de ses outils, produits, applications ou services (Security by Default & by Design).
b) Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité d'accès et d'usage des données qu'il traite pour le compte du responsable de traitement.
c) Tenir à jour une documentation écrite décrivant les mesures de sécurité techniques et organisationnelles mises en œuvre à cet effet.
d) Traiter avec diligence toute demande du responsable de traitement relative à la sécurité des données traitées dans le cadre de la prestation/du marché.
e) Rétablir dans les meilleurs délais la disponibilité et l'accessibilité des données du responsable de traitement en cas d'incident de sécurité.
f) Assurer le stockage des données du responsable de traitement séparément de ses propres données ou des données d'autres clients.
g) Restreindre l'accès aux données faisant l'objet du traitement au seul personnel habilité et autorisé à cet effet, du fait de son travail et de ses fonctions, en limitant l'accès aux données strictement nécessaires à l'accomplissement de leurs tâches.
h) Veiller à ce que les personnes autorisées à traiter les données à caractère personnel :
- s'engagent à respecter la confidentialité et soient soumises aux dispositions du cahier des clauses administratives concernant la confidentialité et le secret professionnel ;
- reçoivent une formation nécessaire en matière de protection des données à caractère personnel.
i) Ne prendre aucune copie des documents et supports d'information confiés par le responsable de traitement, sauf si ladite copie est indispensable à la réalisation de la prestation.
j) Ne pas utiliser, ni communiquer les documents et informations traités à des finalités autres que celles définies par la présente prestation/ le présent marché.

k) Prendre toutes les mesures permettant d'éviter une utilisation détournée ou frauduleuse des données en cours d'exécution de la prestation/du marché.
Le cas échéant, le sous-traitant s'engage par ailleurs à mettre en œuvre les mesures de sécurité prévues par le code de conduite auquel il a adhéré ou la certification dont il se targue.
Toute modification importante des mesures de sécurité mises en place par le sous-traitant doit être documentée et présentée au responsable de traitement pour évaluation. Elles ne peuvent en aucun cas réduire le niveau de sécurité des données pendant la durée du marché.

Article 17 - Mesures de sécurité spécifiques

Le titulaire s'engage à mettre en œuvre les mesures de sécurité spécifiques suivantes (à adapter en fonction du risque) :
- le chiffrement des sauvegardes des données à caractère personnel ;
- le chiffrement des données à caractère personnel en transit ;
- le chiffrement des données à caractère personnel au sein des bases de données ;
- la pseudonymisation des données à caractère personnel ;
- un dispositif de détection des violations de données à caractère personnel ;
- la mise à disposition des traces de connexion aux données traitées pour le compte du responsable de traitement au cours des six derniers mois ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
- etc.

Article 18 - Tests de sécurité

En cas de service exposé sur Internet, le sous-traitant autorise également le responsable de traitement à effectuer ou à faire effectuer des tests de sécurité pour vérifier que les systèmes du sous-traitant ne sont pas vulnérables (par exemple du fait d'un défaut de configuration ou d'un défaut de mise à jour) et détecter tout changement susceptible d'exposer les données à des risques d'intrusion.
Par ailleurs, la caf du Val-de-Marne peut procéder à toute investigation sur Internet permettant de détecter des violations de données à caractère personnel avérées.

Article 19 - Vérification du respect des obligations du sous-traitant

La caf du Val-de-Marne se réserve le droit d'effectuer ou de faire effectuer en son nom et pour son compte, toute vérification qui lui paraîtrait utile pour constater le respect des obligations mentionnées dans la présente annexe, notamment par la réalisation d'audits, y compris des inspections et des tests de sécurité.
Le titulaire coopèrera pleinement à ces audits et s'engage notamment à autoriser le responsable de traitement ou les tiers qu'il a mandatés, à accéder, sans limitation, à l'ensemble des informations nécessaires à l'accomplissement de leur mission, aux environnements physiques et techniques, aux registres et systèmes d'informations, au personnel, ou encore aux sites ou locaux à partir desquels le sous-traitant délivre les prestations visées dans la présente annexe.
Sans préjudice de cette faculté du responsable de traitement, le sous-traitant lui exposera au moins une fois par an les résultats synthétiques des contrôles qu'il met régulièrement en œuvre afin de vérifier le caractère conforme et suffisant des mesures techniques et organisationnelles de sécurité prises.

La caf du Val-de-Marne pourra prononcer la résiliation immédiate du marché, sans indemnité en faveur du sous-traitant, en cas de violation du secret professionnel ou de non-respect des obligations précitées. La responsabilité du sous-traitant peut également être engagée sur le fondement des articles 226-5 et 226-17 du code pénal.

Article 20 - Durée de la prestation et devenir des données à caractère personnel.

L'autorisation donnée par le responsable de traitement au sous-traitant pour effectuer les traitements prévus le cadre de la prestation est valable pour toute la durée du contrat.
À l'issue de la prestation, suivant les instructions du responsable de traitement, au terme de ce marché, le sous-traitant s'engage à supprimer toutes les données à caractère personnel au terme du marché, et détruire les copies existantes dans ses systèmes d'information à la date de fin du marché, à moins que le droit de l'Union européenne ou le droit français n'exige la conservation des données à caractère personnel : dans ce cas le sous-traitant fournit au responsable de traitement le texte exigeant cette conservation. Une fois les données détruites, le sous-traitant doit justifier par écrit de cette destruction.

Article 21 - Responsabilités

Le titulaire sera tenu responsable en cas de manquement exclusivement imputable à lui et/ou à ses sous-traitants ultérieurs à leurs obligations en vertu du présent accord, du rgpd et de la loi informatique et libertés. À ce titre, le titulaire s'engage à indemniser le responsable du traitement pour tout dommage direct subi par ce dernier.

Article 22 - Points de contact

- Les coordonnées du délégué à la protection des données du sous-traitant ou de la personne en charge de la protection des données sont les coordonnées du représentant de l'entreprise signataire de l'acte d'engagement du présent marché.
- Les coordonnées de la personne intervenant pour prendre en charge tout incident de sécurité sont les coordonnées de l'interlocuteur signataire de l'acte d'engagement

Les coordonnées du délégué à la protection des données de la caf du Val-de-Marne sont les suivantes :

Délégué à la protection des données mutualisé
Mission de l'Analyse de la Conformité Informatique et Libertés et de la Sécurité du Système d'Information (Macssi)
32 avenue de la Sibelle – 75685 Paris Cedex 14
protection-dp@cnaf.fr