**MARCHE PUBLIC DE TECHNIQUES DE L’INFORMATION**

**ET DE LA COMMUNICATION**



FOURNITURE DE PRESTATIONS DE CONCEPTION, REALISATION ET MAINTENANCE D’APPLICATIONS METIERS POUR LA DSI DE LA BRANCHE RECOUVREMENT DU REGIME GENERAL DE LA SECURITE SOCIALE

PROCEDURE N° P2524-AOO-DSI

Annexe au CCAP

Sous-traitance de traitement de Données à Caractère Personnel

Dans le cadre du présent accord-cadre, le Titulaire est amené à traiter des données à caractère personnel pour le compte de l’ACOSS. A ce titre, les Parties déclarent que le Titulaire agit en tant que sous-traitant au sens de l’article 4-8) 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 (règlement général sur la protection des données), ci-après le « Règlement » ou « RGPD ». De son côté, l’ACOSS agit en tant que responsable de traitement au sens de l’article 4-7) dudit Règlement.

un traitement de données à caractère personnel dans le cadre de la réalisation de prestations (TMA, MCO, développement projets, tests et assistance) pour son compte, pour l’ensemble des applications faisant partie du patrimoine applicatif de la branche Recouvrement.

Toutes les demandes sont tracées via les bons de commande et les outils de ticketing Redmine et/ou Tandem.

Pour ces prestations, en application de RGPD et de la doctrine RGPD de la DSS, par principe, à chaque fois que cela est possible, le titulaire travaillera à partir de données anonymisées ou fictives. Néanmoins, dans le cadre des prestations qui lui sont confiées, le sous-traitant peut être amené ponctuellement à accéder, à consulter ou à traiter, des données personnelles figurant au sein des traitements mis en œuvre par l’Acoss.

Ce document ne couvre pas les situations suivantes :

* Toute réalisation de traitement de masse par le titulaire (migration, transfert …),
* Toute prestation réalisée hors du périmètre géographique de l’Union Européenne.

Pour ces situations le DPO sera sollicité pour mettre en œuvre les procédures adaptés (clause ad ‘hoc, CCT …).

En conséquence de ces éléments, le traitement de données à caractère personnel n’est pas l’objet principal du présent marché.

Dans cette hypothèse, les données personnelles concernées sont soumises aux clauses de confidentialité stipulées au cahier des clauses administratives particulières de l’accord-cadre et aux articles 4 et 5 de la présente annexe et le sous-traitant s’engage à détruire l’intégralité des données transmises ou accédées pour permettre le traitement d’un incident dès la fin de son intervention.

Au titre de l’exécution de l’accord-cadre, les données personnelles des agents du titulaire sont les données relatives aux identifiants de connexion (nom, prénom et adresse mail) aux plateformes.

**Article 1 - Description du ou des traitement(s) des données à caractère personnel**

Le Titulaire est autorisé à traiter pour le compte de l’ACOSS les données à caractère personnel nécessaires pour fournir des prestations d’assistance à Maîtrise d’Œuvre.

La nature des opérations réalisées sur les données est :

* L’accès si nécessaire ;
* Développements, assistance et réalisation de tests dans le cadre de la conduite de projets.

Les finalités du traitement sont :

* Maintenir en condition opérationnelle les outils informatiques et infrastructures,
* Recettage des applications,
* Traiter (instruire, évaluer, résoudre) les demandes et/ou les incidents, techniques et fonctionnels.

Les principales catégories de données à caractère personnel traitées sont :

* Données d'identification : Nom, prénom, date et lieu de naissance, âge, sexe, adresse personnelle,
* Vie personnelle : Situation familiale, exceptionnellement enfants,
* Vie professionnelle : N° compte cotisant, raison sociale, adresse professionnelle, fonction, emploi, diplômes, type de contrat de travail,
* Données d'ordre économique et financier : Chiffre d’affaires, revenus, salaires, cotisations, dettes, procédures (contentieuses contrôles) RIB,
* Données de connexion : Ponctuellement adresse IP, logs,
* Données de localisation : Néant,
* Internet : Ponctuellement cookies, traceurs, données de navigation, mesures d’audience,
* Données sensibles :
* Ponctuellement NIR,
* Exceptionnellement infractions, opinions syndicales, données biométriques

Les catégories de personnes concernées sont :

* Cotisants,
* Salariés branche ou hors branche,
* Ponctuellement partenaires.

Si le titulaire est amené à conserver des données, leur durée de conservation correspond à la durée du contrat allongée d’une période de 3 mois supplémentaires pour permettre au Titulaire de s’assurer qu’aucune copie des données existe dans son système d’informations.

**Article 2 - Obligations du Titulaire vis-à-vis de l’ACOSS**

Dans le cadre du présent marché subséquent, le Titulaire s’engage à traiter les données uniquement pour la ou les finalités des traitements mentionnées à l’article précédent et qui lui sont sous-traitées. A ce titre, il s’abstient de tout usage de ces données à son profit ou au profit de tiers, y compris à des fins commerciales.

En outre, le Titulaire s’engage à ne traiter les données à caractère personnel que sur la base et conformément aux instructions documentées de l’ACOSS.

Dans l’hypothèse où le RGPD, le droit européen ou le droit français viendrait en contradiction avec les instructions de l’ACOSS ou ne permettrait pas au Titulaire de traiter les données à caractère personnel conformément auxdites instructions, le Titulaire devra en informer l’ACOSS sans délai, et avant de procéder à tout traitement. Dans un tel cas, le Titulaire s’engage à rencontrer à l’ACOSS aux fins de trouver la solution la plus adaptée au regard du marché subséquent et des droits et libertés de la personne concernée. En outre, le Titulaire se porte fort envers l’ACOSS du respect, par ses collaborateurs autorisés à traiter les données à caractère personnel, de la plus stricte confidentialité concernant les données à caractère personnel traitées en exécution du présent marché subséquent. L’ensemble de ces informations sont considérées comme des Informations Confidentielles au sens de l’article « Confidentialité » et sont couvertes par les droits et obligations qui y sont stipulés. Le Titulaire garantit à l’ACOSS qu’il a mis en place et maintient toutes les mesures nécessaires pour préserver et faire respecter par ses collaborateurs la confidentialité des données à caractère personnel.

Ainsi, le Titulaire ne doit rendre accessibles et consultables les données à caractère personnel qu’aux seuls collaborateurs du Titulaire dûment autorisés, en raison de leurs fonctions et qualités, pour traiter les données à caractère personnel dans la stricte limite de ce qui leur est nécessaire à l’accomplissement de leurs fonctions. Le Titulaire déclare avoir dûment formé le personnel concerné en matière de protection des données à caractère personnel.

Le Titulaire s’engage à prendre en compte, s’agissant de ses outils, produits, application et/ou services, les principes de protection des données dès la conception et de protection des données par défaut.

Enfin, le Titulaire déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte de l’ACOSS comprenant :

* Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et du délégué à la protection des données,
* Les catégories de traitements effectuées pour le compte de l’ACOSS,
* 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,
* 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 les 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.

**Article 3 - Obligations de l’ACOSS vis-à-vis du Titulaire**

L’ACOSS s’engage à, en sa qualité de responsable du traitement :

* Fournir au Titulaire les données visées à l’article « description du traitement(s) des données à caractère personnel »,
* Documenter par écrit les instructions concernant le traitement des données par le Titulaire,
* 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 Titulaire,
* Superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire.

**Article 4 - Assistance du Titulaire dans le cadre du respect par l’ACOSS de ses obligations**

Le Titulaire s’engage à apporter toute l’assistance nécessaire à l’ACOSS dans le cas où l’ACOSS mène, pendant la durée du marché subséquent, une analyse d’impact relative à la protection des données à caractère personnel au sens de l’article 35 du Règlement.

Il apportera également assistance à l’ACOSS pour la réalisation de la consultation préalable de l’autorité de contrôle.

**Article 5 - Sécurité des données à caractère personnel**

Le Titulaire garantit à l’ACOSS qu’il a mis en place et qu’il maintient en vigueur et à jour, pendant toute la durée du marché subséquent, toutes les mesures de sécurité de nature technique et organisationnelle visant à assurer la sécurité des données à caractère personnel, de manière à les préserver de toute destruction, perte, altération, divulgation et accès non-autorisés, que ces actes soient d’origine accidentelle ou illicite.

En sus des mesures de sécurité en place antérieurement à l’entrée en vigueur du marché subséquent, le Titulaire devra mettre en œuvre toutes les mesures demandées par l’ACOSS, notamment :

* 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 les 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.

Les Parties identifieront, pendant toute la durée du marché subséquent, toute mise à jour ou modification nécessaire desdites mesures de sécurité notamment aux fins de répondre à toute nouvelle menace ou toute évolution de l’état de l’art ou de la réglementation.

Le Titulaire s’engage à mettre en œuvre les mesures de sécurité prévues au sein du PAS.

**Article 6 - Droit d’information des personnes concernées**

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

**Article 7 - Exercice des droits des personnes**

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 à [informatiqueetlibertes.acoss@acoss.fr].

**Article 8 - Notification des violations de données à caractère personnel**

Le Titulaire notifie à l’ACOSS toute violation de données à caractère personnel dans un délai maximum de douze (12) heures après en avoir pris connaissance. Cette notification doit être faite au délégué à la protection des données et doit être accompagnée de toute documentation utile afin de permettre à l’ACOSS, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente et aux personnes concernées selon la gravité de l’atteinte.

**Article 9 - Sous-traitance**

Toute opération de sous-traitance envisagée par le Titulaire doit être effectuée dans les conditions de l’article « Sous-traitance » de l’accord-cadre.

En outre, dans cette hypothèse, le Titulaire s’engage à communiquer clairement les activités de traitement sous-traitées.

Le sous-traitant est tenu de respecter les obligations de la présente annexe. Il appartient au Titulaire de s’assurer que le sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD. Si le sous-traitant ne respecte pas ses obligations en matière de protection des données, le Titulaire demeure pleinement responsable devant l’ACOSS de l’exécution par le sous-traitant de ses obligations.

**Article 10 - Données à caractère personnel en fin de marché subséquent**

Si le titulaire est amené à stocker des données personnelles, au terme du marché subséquent, quelle qu’en soit la cause, le Titulaire s’engage à détruire toutes les données à caractère personnel ainsi que toutes les copies existantes dans les systèmes d’information du Titulaire. Une fois détruites, le Titulaire doit justifier par écrit de la destruction.

**Article 11 - Documentation et audit**

Le Titulaire met à la disposition de l’ACOSS la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d’audits, y compris des inspections, par l’ACOSS ou un autre auditeur qu’elle a mandaté, et contribuer à ces audits.

**Article 12 - Manquement du Titulaire**

En cas de non-respect par le Titulaire des obligations visées dans la présente annexe et à l’article 13 de l’accord-cadre, et indépendamment des sanctions pénales et administratives encourues, l’ACOSS pourra décider de résilier le marché subséquent aux torts exclusifs du Titulaire, sans ouvrir droit à indemnités, à quelque titre que ce soit.