Annexe / Avenant / Convention de sous-traitance relatif/ve à la protection des données à caractère personnel

Sommaire

Préambule X

Article 1 : Description du traitement de données à caractère personnel X

Article 2 : Obligations des contractants X

2.1. Les engagements du sous-traitant vis-à-vis du responsable du traitement X

2.2. Responsabilité des parties X

2.3. Droit applicable et juridiction X

Article 3 : Droit à l'information des personnes concernées X

Article 4 : Exercice des droits des personnes concernées X

Article 5 : Notification des violations de données à caractère personnel X

Article 6 : Durée de conservation des données à caractère personnel X

Article 7 : Délégué à la protection des données X

Article 8 : Registre des activités de traitement X

Article 9 : Contrôle de conformité du sous-traitant X

Article 10 : Sous-traitance ultérieure X

Article 11 : Transfert hors de l'Union européenne ou de l'Espace économique européen X

Article 12 : Durée et date d'effet X

Le présent document contractuel est signé entre :

La CARSAT Sud-Est (ci-après dénommée « Responsable du traitement »)
Organisme de Sécurité Sociale immatriculé au Registre du Commerce et des Sociétés de Marseille sous le numéro SIRET n°775 559 115 00016 (Organisme privé gérant une mission de service public),
dont le siège est situé : 35 rue George, 13386 MARSEILLE Cedex 20
représentée par son Directeur, Monsieur Vincent VERLHAC.

Et,

X **(ci-après dénommé « Sous-traitant »)**
X,
dont le siège est situé : X
représentée par son Directeur, X.

Ci-après désignées collectivement « les Parties ».

Préambule

Les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier :

- Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, ci-après « RGPD » ;
- La Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 susmentionnée.

Les parties reconnaissent que :

- Les termes spécifiques employés dans le présent document contractuel le sont tels que définis par le RGPD ;
- Le présent document contractuel se substitue à toute clause applicable en matière de protection des données à caractère personnel pouvant se trouver dans un autre document contractuel liant les Parties pour le même objet de sous-traitance. En cas de contradiction, les Parties conviennent expressément que le présent document contractuel prévaut ;
- La Carsat Sud-Est est le responsable du traitement, au sens de l'article 4,7°) du RGPD ;
- X agit en qualité de sous-traitant du responsable du traitement, au sens de l'article 4, 8°) du RGPD ;
- L'ensemble des données mis à dispositions par le responsable du traitement, ainsi que l'ensemble des données qui seraient collectées et enrichies par le sous-traitant, demeure la seule propriété pleine et entière du responsable du traitement ;
- Le non-respect des obligations décrites ci-dessous peut entrainer la résiliation du document contractuel avec effet immédiat aux torts exclusifs du sous-traitant par notification écrite ;
- Le présent document contractuel ne peut être modifié, sauf par écrit signé par les représentants dûment autorisés de chacune des Parties.

Le présent document contractuel a pour objet de définir les conditions dans lesquelles le traitement tel que défini ci-après est réalisé par le sous-traitant pour le compte du responsable du traitement.

<u>Article 1</u> : Description du traitement de données à caractère personnel

Conformément à l'article 28 relatif au « sous-traitant », alinéa 3, du RGPD, le document contractuel qui lie le sous-traitant au responsable du traitement définit l'objet, la durée et la finalité du traitement, ainsi que le type de données à caractère personnel et les catégories de personnes concernées par le traitement de leurs données.

La ou les finalité(s) du traitement sont [spécifier les finalités poursuivies par le traitement des données] <u>ou</u> [sont décrites à l'article X de la convention X <u>ou</u> dans l'annexe X de la convention X].

Le traitement réalisé par le sous-traitant consiste en [décrire des opérations de traitement réalisées par le sous-traitant sur les données] <u>ou</u> [sont décrites à l'article X de la convention X <u>ou</u> dans l'annexe X de la convention X].

Les catégories de personnes concernées sont [préciser le profil des personnes dont les données sont sous-traitées] <u>ou</u> [sont décrites à l'article X de la convention X <u>ou</u> dans l'annexe X de la convention X].

Les données à caractère personnel sous-traitées sont [*remplir le tableau ci-dessous*] ou [sont décrites à l'article X de la convention X ou dans l'annexe X de la convention X].

Catégories des données	Données
Identification *Nom, prénom, adresse, numéro de téléphone, identifiant, photo, enregistrement sonore, état civil, identité, identité conjoint, identité enfants, sexes, dates de naissance, nationalité*	
Coordonnées de contact *Adresse postale, adresse mail, téléphone fixe, téléphone portable*	
Vie personnelle *Situation maritale, nombre d'enfants ou de personnes âgées à charge, habitudes de vie, hobbys*	
Vie professionnelle *Profession, employeur, CV, diplôme, formation, distinction, direction, UO, EAEA/EP, numéro d'agent, coefficient, nature du document contractuel*	
Information d'ordre économique et financier *Coordonnées bancaires, RIB, revenue, situation fiscale, pension de retraite, pension de réversion, aides sociales, aides au logement*	
Données de connexions et traçabilité *Log, horodatage, adresse IP, traçabilité des actions, journaux d'évènements, cookies fonctionnels*	
Données de localisation *Données GPS, badge*	
Autres *Zones de commentaires libres, bloc-notes*	
Données particulières et sensibles *Le niveau de sécurité technique et organisationnel doit être adapté à la sensibilité des données sous-traitées.*	
Identifiants nationaux *NIR, NIR d'attente (NIA)*	
Santé, biométrie et génétique *Handicap, analyses, forme physique, pathologies*	
Vie et orientation sexuelle *Homosexuel, bisexuel, pratiques sexuelles*	
Infractions, condamnations ou mesure de sûreté *Délits, fraudes, dépôts de plainte, casier judiciaire, jugements, contraventions*	
Origine raciale ou ethnique *Couleurs de peau, traditions*	
Opinions politiques, philosophiques, convictions religieuses ou appartenance syndicale	

<u>Article 2</u> : Obligations des contractants

2.1. Les engagements du sous-traitant vis-à-vis du responsable du traitement

Conformément notamment au respect de l'article 28 « Sous-traitant » et 32 « Sécurité du traitement » du RGPD, le sous-traitant s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) définies ci-dessus ;

- Ne traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, 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 le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

- Prendre toutes les mesures requises en vertu de l'article 32 du RGPD et en adéquation avec la sensibilité des données sous-traitées ;

- Assurer la sécurité des flux de données et à utiliser des outils d'échange sécurisés ;

- S'assurer que tous les systèmes, les services et les produits utilisés dans le cadre du traitement de données à caractère personnel sont conformes à la réglementation sur la protection des données ;

- Respecter les conditions de licence applicables et toutes les politiques qui lui sont notifiées lorsqu'il a accès ou utilise tout logiciel, matériel, système ou équipement fournis par le Responsable du traitement ou l'un de ses sous-traitants ;

- Ne divulguer aucune donnée à caractère personnel à un tiers sans l'accord écrit préalable du responsable du traitement ;

- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent document contractuel :
  - Soient soumises à une obligation contractuelle appropriée de confidentialité ;
  - Reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

- Aider le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, à savoir notamment notifier à l'autorité de contrôle une violation de données à caractère personnel, communiquer à la personne concernée une violation de données à caractère personnel, réaliser une analyse d'impact relative à a protection des données (AIPD) et consulter préalablement la CNIL, compte tenu de la nature du traitement et des informations à sa disposition ;

- Mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;

- Informer le responsable du traitement s'il reçoit une plainte, un avis, une communication ou une mise en demeure d'une Autorité de régulation ou de contrôle qui concerne

directement ou indirectement le traitement sous-traité ou sa non-conformité à la réglementation sur la protection des données à caractère personnel ;

- Informer le responsable du traitement si une instruction constitue une violation du droit en vigueur relatif à la protection des données à caractère personnel ;

- Informer par écrit le responsable du traitement si une opération du traitement des données (hébergement, transfert, etc.) est réalisé hors de l'Union européenne ou de l'Espace économique européen et à assurer un niveau de protection des données suffisant et approprié conformément au chapitre V du RGPD et aux préconisations de la Commission Nationale Informatique et Libertés (CNIL) ;

- Déclarer ses éventuels sous-traitants actuels et ultérieurs au responsable du traitement, en cas de recours à des sous-traitants pour la mise en œuvre des activités de traitement sous-traitées, et à s'assurer et exiger par document contractuel que ces derniers, ainsi que leurs potentiels sous-traitants, présentent le même niveau de garantie que celui exigé dans le présent document contractuel. Le sous-traitant demeure pleinement responsable devant le responsable du traitement de l'exécution par ses sous-traitants et leurs sous-traitants de leurs obligations ;

- Appliquer la réglementation en vigueur relative à la gestion des cookies, si la sous-traitance concerne le développement ou l'administration d'un site ou d'une application recourant au dépôt de cookies ;

- Appliquer les instructions du responsable du traitement, et notamment en matière de conservation des données à caractère personnel.

2.2. Responsabilité des parties

Les contractants conviennent que leur responsabilité pourra être engagée en cas de préjudice résultant d'une violation de la réglementation en vigueur applicable au traitement de données à caractère personnel.

Le Responsable du traitement ne saurait voir sa responsabilité engagée, notamment lorsque le sous-traitant agit en dehors de ses engagements contractuels et des instructions licites du responsable du traitement.

Dans ce cadre, le sous-traitant indemnisera le responsable du traitement de tous les frais, les dépenses (y compris les frais juridiques, les autres frais professionnels et les coûts liés à l'information des personnes concernées et des Autorités de régulation de toute violation), les pertes, les dommages et autres responsabilités de toute nature (contractuelles, délictuelles ou autres), découlant de ou en relation avec une violation du présent document contractuel, de la réglementation ou de données, subies ou encourues par le responsable du traitement, ses représentants, ses agents, ses sous-traitants et ses destinataires autorisés. La responsabilité du sous-traitant sera illimitée et ne sera pas soumise à un plafond de responsabilité éventuellement défini dans d'autres clauses du document contractuel liant les Parties.

En application des articles 82.4 et 82.5 du RGPD, le responsable du traitement dispose de la faculté d'engager une action récursoire à l'encontre du sous-traitant ayant pris part à l'exécution des traitements de données à caractère personnel pour lesquels un dommage a été causé aux personnes concernées.

2.3. Droit applicable et juridiction

Le présent document contractuel sera régi et interprété conformément à la loi française et tout litige découlant de ou en relation avec le présent document contractuel sera soumis à la juridiction exclusive des tribunaux français, auxquelles chacune des Parties se soumet irrévocablement.

Avant toute action contentieuse, les Parties chercheront, de bonne foi, à régler à l'amiable leurs différends relatifs à la validité, l'interprétation, l'exécution ou l'inexécution, l'interruption, la résiliation ou la dénonciation du présent document contractuel ainsi qu'à la cessation partielle ou totale des relations commerciales entre les Parties et ce, pour quelques causes et sur quelques fondements que ce soient. Les Parties pourront se réunir afin de confronter leurs points de vue et effectuer toutes les constatations utiles pour leur permettre de trouver une solution au conflit qui les oppose.

Article 3 : Droit à l'information des personnes concernées

[Au choix de la direction acheteuse en accord avec le DPO]

Option A (par défaut)
Il appartient au responsable du traitement de fournir l'information aux personnes concernées par le traitement de leurs données conformément aux articles 12, 13 et 14 du RGPD.

Option B
Le sous-traitant met en œuvre l'information aux personnes concernées relative au traitement de leurs données qu'il réalise pour le compte du responsable du traitement, conformément aux articles 12, 13 et 14 du RGPD.

La mention d'information sur la protection des données et son support de diffusion doivent être préalablement validés par le responsable du traitement.

Article 4 : Exercice des droits des personnes

Le sous-traitant s'engage à aider le responsable du traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées dans le délai imposé par la loi, conformément chapitre III du RGPD, par la mise en œuvre de mesures techniques et organisationnelles.

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, ce dernier doit adresser ces demandes dès réception par courrier électronique à : informatiqueetlibertes@carsat-sudest.fr.

Le sous-traitant s'engage à ne pas divulguer aux personnes concernées de données sans avoir préalablement consulté et obtenu l'accord écrit du responsable du traitement.

Article 5 : Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel, réelle ou potentielle, accidentelle ou non, affectant les données à caractère personnel objet du présent document contractuel de sous-traitance dans un délai maximum de 48 heures après en avoir pris connaissance, en l'adressant au délégué à la protection des données du responsable du traitement par message électronique à l'adresse mail suivante : informatiqueetlibertes@carsat-sudest.fr et par courrier avec accusé de réception à l'adresse

postale suivante : Monsieur Le Directeur Général de la Carsat Sud-Est, à l'attention du DPO - 35, Rue George - 13386 Marseille Cedex 20.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable du traitement d'apprécier et limiter la gravité des impacts pour les personnes concernées et de déterminer s'il est nécessaire d'une part, de notifier cette violation à l'autorité de contrôle compétente et d'autre part, de la communiquer aux personnes concernées.

La description de la violation de données à caractère personnel comprend a minima la nature de la violation et des données compromises, les catégories et le nombre approximatif de personnes concernées par la violation, la description des conséquences probables de la violation, les mesures prises ou proposées pour y remédier et 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.

Dans le cas où il n'est pas possible de fournir toutes ces informations en même temps, le sous-traitant les communique de manière échelonnée sans retard indu.

Le sous-traitant se tient à la disposition du responsable du traitement et reste joignable directement jusqu'à la résolution de la violation de données, y compris pour prendre les mesures nécessaires afin d'atténuer les éventuelles conséquences négatives et remédier à toute autre violation ultérieure.

Article 6 : Durée de conservation des données à caractère personnel

Option A et B

Dans le cadre de la réalisation du traitement de données, si le sous-traitant est amené à stocker ou gérer l'hébergement des données à caractère personnel, il s'engage à appliquer les durées de conservation et d'accès déterminées par le responsable du traitement. Par défaut, la durée de conservation des données est la durée de l'engagement contractuel.

Au terme de la durée conservation des données, le sous-traitant s'engage à détruire toutes les données à caractère personnel, y compris les éventuelles copies et sauvegardes, sauf s'il y a une clause de réversibilité ou si sur instruction écrite du responsable du traitement, il est demandé que les données soient restituées dans un format exploitable au responsable du traitement ou à un tiers désigné par celui-ci. Le renvoi, le cas échéant, doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant ou sous sa responsabilité.

Une fois détruites, le sous-traitant doit pouvoir certifier, par écrit signé par son représentant légal ou un délégataire, de la destruction de toutes les données.

Option B

La durée de conservation des données traitées par le sous-traitant est […] *(Préciser le délai ou décrire l'évènement déclencheur de la suppression des données ou Retirer la ligne)*.

Article 7 : Délégué à la protection des données

Le sous-traitant communique au responsable du traitement les coordonnées génériques 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 de son interlocuteur référent en matière de protection des données à caractère personnel.

Les coordonnées du délégué à la protection des données du responsable du traitement est l'adresse générique suivante : informatiqueetlibertes@carsat-sudest.fr

Les coordonnées du délégué à la protection des données ou du référent en matière de protection des données à caractère personnel du sous-traitant est : [A COMPLETER]

Article 8 : Registre des activités de traitement

Le sous-traitant, comptant au moins 250 employés ou effectuant un traitement susceptible de comporter un risque pour les droits et libertés des personnes ou effectuant un traitement non-occasionnel ou effectuant un traitement portant sur les catégories particulières de données visées à l'article 9 ou sur des données visées à l'article 10 du RGPD, déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement comprenant au moins :

- Le nom et les coordonnées du responsable du traitement pour le compte duquel 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 du responsable du traitement ;
- 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 européen 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 visées à l'article 32 du RGPD.

Article 9 : Contrôle de conformité du sous-traitant

Le responsable du traitement peut auditer ou faire auditer les mesures de sécurité, de confidentialité et de conformité à la réglementation sur la protection des données à caractère personnel mises en place par le sous-traitant afin de vérifier qu'il se conforme à ses engagements.

A cette fin, le sous-traitant accorde au responsable du traitement tout accès ou information nécessaire à l'accomplissement du contrôle de conformité et à la revue de tous les fichiers et autres documentations relatifs au traitement des données à caractère personnel sous-traité.

Le sous-traitant s'engage à ses frais auprès du responsable du traitement à fournir sur demande et sans délai les informations que le responsable du traitement peut raisonnablement demander pour confirmer que le sous-traitant agit conformément à la réglementation sur la protection des données et à ses instructions écrites.

Le responsable du traitement pourra donner au sous-traitant un préavis d'au moins sept jours en vue de contrôler ou de désigner des représentants pour inspecter toutes les installations, équipements, dossiers, documents et données en lien avec le traitement des données sous-traitées.

Le sous-traitant convient que si des vulnérabilités de système ou de processus sont découvertes lors d'un audit ou d'une inspection effectuée ou de toute information fournie, il

s'engage à corriger ces vulnérabilités dans le délai fixé par le responsable du traitement à ses seuls frais.

<u>Article 10</u> : Sous-traitance ultérieure

Le sous-traitant peut faire appel à un sous-traitant (ci-après dénommé « le Sous-Traitant Ultérieur ») pour mener des activités de traitement spécifiques dans le cadre du présent document contractuel. Dans ce cas, il doit obligatoirement informer préalablement et par écrit le responsable du traitement de tout changement envisagé concernant l'ajout ou le remplacement de Sous-Traitants Ultérieurs.

Cette information doit indiquer clairement les activités de traitements sous-traitées, l'identité et les coordonnées du Sous-Traitant Ultérieur et les dates du document contractuel de Sous-Traitance. Le Responsable du traitement dispose d'un délai minimum de trois semaines à compter de la date de réception de cette information pour l'accepter ou le refuser au regard de son niveau de conformité à la réglementation en vigueur en matière de protection des données à caractère personnel. Cette sous-traitance ultérieure ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant ce délai convenu.

Le Sous-Traitant Ultérieur est tenu de respecter les obligations du présent document contractuel pour le compte et selon les instructions du responsable du traitement. Il appartient au sous-traitant de s'assurer que le Sous-Traitant Ultérieur 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 réglementation sur la protection des données à caractère personnel. Le sous-traitant conclut par ailleurs avec le Sous-Traitant Ultérieur un document contractuel reprenant les obligations prévues.

Dans tous les cas, si le Sous-Traitant Ultérieur ne remplit pas ses obligations en matière de protection des données à caractère personnel, le sous-traitant demeure pleinement responsable devant le responsable du traitement de l'exécution par le Sous-Traitant Ultérieur de ses obligations.

Le responsable du traitement se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour s'assurer du respect des obligations du présent document contractuel tant par le sous-traitant que par ses Sous-Traitants Ultérieurs éventuels.

Le responsable du traitement se réserve le droit de révoquer son accord de sous-traitance ultérieure dès lors que le Sous-Traitant Ultérieur concerné ne respecte pas les obligations équivalentes à celles imposées au sous-traitant en vertu du présent document contractuel, ou si les actions ou omissions du Sous-Traitant Ultérieur sont susceptibles de violer la réglementation sur la protection des données à caractère personnelle ou de placer le responsable du traitement en situation de violer cette réglementation.

<u>Article 11</u> : Transfert hors de l'Union européenne ou de l'Espace économique européen

Le sous-traitant est tenu d'informer par écrit le responsable du traitement si une opération du traitement des données (hébergement, transfert, etc.) est réalisé hors de l'Union européenne ou de l'Espace économique européen et d'assurer un niveau de protection des données suffisant et approprié conformément au chapitre V du RGPD et aux préconisations de la Commission Nationale Informatique et Libertés (CNIL).

Cette information doit indiquer clairement les activités de traitements réalisées hors de l'Union européenne ou de l'Espace économique européen, l'identité des sous-traitants ultérieurs

concernés, le cas échéant, et leur nationalité, les pays concernés et leur niveau d'adéquation reconnu par la Commission européenne, les catégories de données concernées, les catégories de personnes concernées et les mesures techniques, organisationnelles et contractuelles de protection nécessaires et prévues par le sous-traitant, conformément aux recommandations 01/2020 du Comité européen de la protection des données (CEPD) sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'Union européenne.

Le traitement de données à caractère personnel hors de l'Union européenne ou de l'Espace économique européen ne peut être effectué sans l'accord préalable et écrit du responsable du traitement. L'accord peut être soumis à des conditions que le responsable du traitement juge appropriées et selon sa discrétion absolue.

Le responsable du traitement se réserve le droit de révoquer son accord de transfert hors de l'Union européenne ou de l'Espace économique européen en cas de risque pour la protection des données à caractère personnel sous-traitées jugé à la discrétion du responsable du traitement.

Article 12 : Durée et date d'effet de l'accord

Le présent accord prend effet à la date de sa signature par les Parties et prendra fin [A PRECISER].

Fait à Marseille en deux exemplaires, le XX/XX/XXX,

Pour la Carsat Sud-Est	Pour X
Le Directeur **Vincent VERLHAC**	XXXXXXXXXXX **XXXXXXX XXXXXXXX**