

ANNEXE Sous-Traitance RGPD

1. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cas d'un traitement de données à caractère personnel du pouvoir adjudicateur par le Prestataire pour le présent Contrat, les Parties reconnaissent que les entités du Groupe Action Logement sont le Responsable de traitement, chacune sur leur périmètre, et le Prestataire est le Sous-traitant.

Dans le cadre de leurs relations contractuelles, 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 applicable à compter du 25 mai 2018 (ci-après, « **le règlement européen sur la protection des données** »).

2. Définitions

Tous les mots commençant par une majuscule dans cette Annexe sont réputés avoir le même sens que celui retenu par le RGPD et le Contrat.

Donnée à caractère personnel : Toute information identifiante directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

Traitement de données à caractère personnel : Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...).

Responsable de traitement : Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Sous-traitant au sens du RGPD : désigne la personne physique ou morale, l'autorité publique, le service ou l'organisme qui traite des données à caractère personnel pour le compte du Responsable de traitement.

3. Description du traitement

Le Sous-traitant sera amené à traiter des données à caractère personnel dans le cadre des traitements décrits ci-après en annexe. Le Responsable de traitement pourra modifier à tout moment la description de ces traitements et en notifiera le Sous-traitant.

4. Date d'entrée en vigueur et durée de l'annexe

La présente annexe entrera à compter de sa signature par les deux Parties pour une durée expirant à la date de fin du contrat principal convenu entre les parties.

5. Obligations du Sous-traitant

5.1 Respect des instructions du Responsable de traitement

Il incombe au Sous-traitant de traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet de la sous-traitance.

En outre, le Sous-traitant s'engage à traiter les données conformément aux instructions documentées du Responsable de traitement.

Si le Sous-traitant considère qu'une instruction constitue une violation du règlement européen 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 Responsable de traitement.

En outre, si le Sous-traitant est tenu de procéder à un transfert de données vers un pays tiers 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 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.

5.2 Privacy by design et by default

Le sous-traitant s'engage à prendre en compte, au titre du traitement de Données personnelles, les principes de protection des Données dès la conception et de protection des Données par défaut.

5.3 Garantie de confidentialité

Le Sous-traitant s'engage à garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

Il assure également que toutes les personnes autorisées à traiter les données à caractère personnel s'engagent bien à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

Par ailleurs, le Sous-traitant s'interdit :

- La consultation, le traitement de données autres que celles concernées par les présentes et ce, même si l'accès à ces données est techniquement possible ;
- De divulguer, sous quelque forme que ce soit, tout ou partie des données exploitées ;
- De prendre copie ou de stocker, quelles qu'en soient la forme et la finalité, tout ou partie des informations ou données contenues sur les supports ou documents qui lui ont été confiés ou recueillies par elle au cours de l'exécution des présentes, en dehors des cas couverts par les présentes.

5.4 Obligations de formation du personnel

Le Sous-traitant s'engage à ce que toutes les personnes autorisées à traiter les données à caractère personnel aient bien reçu la formation nécessaire en matière de protection des données à caractère personnel.

A ce titre, il s'engage à faire appliquer dès la conception de ses outils, applications ou services, les principes de protection des données personnelles au sein de son établissement.

5.5 Mise en place d'une sous-traitance

Le sous-traitant ne peut faire appel à un autre sous-traitant ultérieur pour mener des activités de traitement spécifiques qu'après avoir obtenu l'accord préalable, écrit et exprès du Responsable de traitement.

Pour ce faire, le Sous-traitant informe préalablement, dans un délai maximum de trente (30) jours avant la date de recours prévue, et par écrit le Responsable de traitement de l'existence, 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 de sous-traitance.

Dans l'hypothèse où le Sous-traitant aurait été autorisé à sous-traiter les prestations, il s'engage à :

- Informer et signer avec son sous-traitant ultérieur un contrat écrit faisant référence aux présentes, et imposant au sous-traitant les mêmes obligations en matière de protection des données que celles fixées dans la présente ;
- Mettre à la charge de son sous-traitant toute obligation nécessaire pour que soient respectées la confidentialité, la sécurité et l'intégrité des données, et pour que lesdites données ne puissent être ni cédées ou louées à un tiers à titre gratuit ou non, ni utilisées à d'autres fins que celles définies dans la présente ;

- Communiquer au Responsable de traitement concerné une copie du contrat avec son ou ses sous-traitants et à défaut une description des éléments essentiels du contrat, incluant la mise en œuvre des obligations relatives à la protection des données à caractère personnel ;
- Tenir à la disposition du Responsable de traitement concerné une liste du ou des sous-traitants impliqués dans le traitement de données à caractère personnel.

Les données traitées en exécution du contrat ne pourront faire l'objet d'aucune divulgation à des tiers, et ce y compris aux sous-traitants du Sous-traitant, en dehors des cas prévus dans la présente annexe ou de ceux prévus par une disposition légale ou réglementaire.

Lorsque ses sous-traitants ne remplissent pas leurs obligations en matière de protection des données, le Sous-traitant demeure pleinement responsable devant le Responsable de traitement concerné de l'exécution par les sous-traitants de leurs obligations. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

5.6 Transfert hors Union européenne des données à caractère personnel

Pour tout transfert de données à caractère personnel du Responsable de Traitement vers un pays ayant une protection considérée comme non suffisante, non-adéquate ou un pays hors de l'Union Européenne ne disposant d'aucune protection considérée comme adéquate par la Commission Européenne, le Sous-traitant s'engage à obtenir systématiquement l'accord exprès, écrit, spécifique et préalable du Responsable de Traitement et à respecter les dispositions prévues au Chapitre V du RGPD.

Le Sous-traitant s'engage à notifier au Responsable de Traitement son intention de recourir à un prestataire et décrire les flux hors Union Européenne qui seraient mis en œuvre au minimum trois (3) mois avant la date envisagée pour la mise en œuvre des flux, de telle manière à lui permettre de mettre en œuvre les conditions de légalité de ces transferts.

En cas d'autorisation accordée par le Responsable de Traitement, le Sous-traitant s'engage à encadrer ces transferts par le biais de « clauses contractuelles types pour le transfert de données à caractère personnel » en vigueur selon les modalités prévues par décision de la Commission européenne sur la base de l'article 46, paragraphe 2, sauf si le sous-traitant hors union européenne bénéficie d'un autre mécanisme d'encadrement des flux comme par exemple des règles contraignantes d'entreprise.

Le Sous-traitant s'engage à communiquer les mécanismes de transferts de données à caractère personnel au Responsable de Traitement.

Dans l'hypothèse où le Sous-traitant est tenu de procéder à un transfert de données vers un pays tiers 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 Responsable de Traitement de cette obligation juridique avant le traitement.

5.7 Droit d'information des personnes concernées

Il appartient au Responsable de traitement, au moment de la collecte des données, de communiquer aux personnes concernées par les opérations de traitement leur droit d'information.

Nonobstant, dans le cas où le sous-traitant procéderait, au titre du traitement, directement à la collecte des Données personnelles, et après accord préalable du responsable de traitement, le sous-traitant devra, au moment de cette collecte, fournir aux personnes concernées par les opérations de traitement, l'information relative au traitement de Données qu'il réalise, et recueillir leur consentement le cas échéant, conformément à la Réglementation applicable en matière de protection des données personnelles.

La formulation et le format de cette information des personnes concernées doit être convenu avec le responsable de traitement avant la collecte des Données personnelles.

5.8 Modalité d'exercice des droits des personnes

Dans la mesure du possible, le Sous-traitant doit assister le Responsable de traitement à remplir son obligation légale de donner suite aux demandes d'exercice des droits des personnes concernées. Ce droit est décomposé comme suit :

- Droit d'accès aux données ;
- Droit de rectification des données ;
- Droit de suppression des données ;
- Droit d'opposition au traitement des données ;
- Droit à la limitation du traitement ;
- Droit à la portabilité des données ;
- Droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage)
- Droit de se voir notifier toute rectification, effacement de données ou limitation du traitement ainsi que le droit d'être informé sur les destinataires des données les concernant.

Lorsque les personnes concernées exercent auprès du Sous-traitant des demandes d'exercice de leurs droits, le Sous-traitant doit adresser ces demandes dès réception par courrier électronique à la Section opérationnelle de lutte contre les cybermenaces DAS SAJ Paris-Maisons-Alfort (solc.das.saj.paris-maisons-alfort@gendarmerie.interieur.gouv.fr) et au bureau budget administration de la division de l'appui opérationnel de la Région de Gendarmerie d'Ile-de-France (bba.dao.rgif@gendarmerie.interieur.gouv.fr).

Le sous-traitant ne répondra à aucune demande de personnes concernées directement sans l'autorisation préalable et écrite du responsable de traitement et uniquement selon ses instructions.

5.9 Notification des violations de données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance par mail (cf. adresses rappelées supra) et par lettre recommandée avec accusé de réception. Cette notification est

accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Le Sous-Traitant s'engage à collaborer activement avec le Responsable de Traitement pour qu'il soit en mesure de répondre à ses obligations réglementaires et contractuelles.

Selon les cas, le sous-traitant peut être amené à notifier à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

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 du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, 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 le responsable du traitement 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.

Sauf lorsque la loi ou la réglementation applicable le requiert, le sous-traitant ne publiera aucune communication externe, communiqué de presse ou rapport concernant toute violation relative aux Données personnelles sans l'autorisation préalable et écrite du responsable de traitement.

En toute hypothèses, il appartient au responsable de traitement de décider et de procéder s'il y a lieu à une notification de la violation de Données personnelles à l'Autorité de contrôle. Dans l'hypothèse où le responsable de traitement et le sous-traitant seraient tous deux soumis à une obligation de notification à l'Autorité de contrôle (notamment auprès de la CNIL), une coordination devra être assurée entre les le responsable de traitement et le sous-traitant quant à la cohérence du contenu et aux délais des différentes notifications.

5.10 Obligations d'assistance du Sous-traitant

Le Sous-traitant assiste le Responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données concernant notamment les traitements de données « sensibles » ou présentant un risque particulier pour les droits des personnes concernées.

Le Sous-traitant est également tenu de soutenir le Responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

Le sous-traitant s'engage par ailleurs à aider et à assister le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (droit d'accès, rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données) et le cas échéant transmettre au responsable de traitement dans le délai de 7 jours ouvrés à compter de la demande de ce dernier tous les éléments nécessaires.

5.11 Mesures de sécurité

Le Sous-traitant s'engage à prendre toute précaution utile au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données des fichiers et notamment empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès par des tiers non autorisés préalablement.

Le sous-traitant est responsable de la mise en œuvre et du maintien pendant toute la durée du contrat de toutes mesures techniques et organisationnelle appropriées pour protéger les données à caractère personnel, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir le responsable de traitement d'un niveau de sécurité adapté au risque.

A ce titre, le sous-traitant s'engage a minima à mettre en œuvre, sous sa seule responsabilité les mesures suivantes :

- Sécurité liée au personnel,
- Authentification des utilisateurs,
- Gestion des habilitations,
- Traçabilité des accès et des audits,
- Sécurité logique,
- Pollution informatique,
- Gestion de l'exploitation.

Le Sous-traitant s'engage à maintenir ces moyens tout au long de l'exécution du contrat et à défaut, à en informer immédiatement le Responsable de traitement concerné.

5.12 Renvoi des données à la fin du contrat

Au terme de la prestation de services relatifs au traitement de ces données, ou à tout moment sur demande du Responsable du traitement, le Sous-traitant s'engage à renvoyer les données à caractère personnel au Responsable de traitement, ou le cas échéant au Sous-traitant désigné par le Responsable de traitement.

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.

5.13 Information du Délégué à la protection des données (DPO)

Le Sous-traitant communique au Responsable de traitement 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.

Contact Délégué à la Protection des Données :

Section opérationnelle de lutte contre les cybermenaces DAS SAJ Paris-Maisons-Alfort

solc.das.saj.paris-maisons-alfort@gendarmerie.interieur.gouv.fr

5.14 Création d'un Registre des catégories d'activités de traitement

Le Sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement comprenant :

- Le nom et les coordonnées du Responsable de 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, y compris entre autres celles prévues à l'article 4.8 Mesures de sécurité.

5.15 Mise à disposition d'une Documentation et vérifications

Le Sous-traitant met à la disposition du Responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

Ces informations et documents seront conservés et archivés afin de répondre aux demandes d'audit du Responsable de traitement ou, à ses frais, par un tiers de confiance qu'il aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Sous-traitant, ayant une qualification adéquate, et libre de lui fournir les détails de ses remarques et conclusion d'audit.

Sous réserve d'un délai de prévenance d'au moins trente (30) jours calendaires (sauf si une période plus courte est requise pour répondre à une obligation légale ou à la demande d'une autorité gouvernementale), les missions d'audits seront réalisées au moins une fois par an, ou en cas d'évènement majeur ayant une potentielle incidence sur la sécurité et/ou l'intégrité des données du Responsable de traitement.

La participation du Sous-traitant à ces audits ne sera pas facturée au Responsable de traitement.

Les audits doivent permettre une analyse du respect par le Sous-traitant de ses obligations ainsi qu'au titre de la réglementation Informatique et libertés. Ils doivent permettre notamment de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié. Elles peuvent porter sur l'un des domaines suivants :

- application des procédures de sécurité et de sauvegarde des Données Personnelles ;
- contrôle de la sécurité physique et logique des serveurs sur lesquels sont traitées les Données
- traçabilité des flux de Données Personnelles et localisation de leurs sites d'hébergement, de sauvegarde et de traitement.

Les audits seront soumis à toutes les obligations de confidentialité applicables et devront être effectués de manière à minimiser toute perturbation dans l'exécution des services et autres opérations normales par le Sous-traitant.

Dans l'hypothèse où un tel audit révèle des lacunes ou des faiblesses importantes, le Responsable de traitement pourra suspendre la transmission des Données Personnelles au Sous-traitant et mettre fin au Traitement des Données Personnelles par le Sous-traitant, jusqu'à ce que ces problèmes soient résolus.

L'audité s'engage à corriger les anomalies, à ses frais, afin de rendre le Traitement conforme à l'état de l'art du moment et à la Réglementation applicable, sous un délai raisonnable.

En cas de contrôle d'une autorité compétente, les Parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le Sous-traitant en tant que Responsable du traitement, le Sous-traitant fera son affaire du contrôle et s'interdira de communiquer ou de faire état des données à caractère personnel du Responsable de Traitement.

Dans le cas où le contrôle mené chez le Sous-traitant concernerait les traitements mis en œuvre au nom et pour le compte du Responsable de traitement concerné, le Sous-traitant s'engage à en informer immédiatement le Responsable de Traitement et à ne prendre aucun engagement pour elle.

En cas de contrôle d'une autorité compétente chez le Responsable de traitement portant notamment sur les prestations délivrées par le Sous-traitant, cette dernière s'engage à coopérer avec le Responsable de traitement et à lui fournir toute information dont cette dernière pourrait avoir besoin ou qui s'avèrerait nécessaire.

6. Obligations du Responsable de traitement envers le Sous-traitant

Le Responsable de traitement s'engage à :

- Fournir au Sous-traitant les données visées à l'article 3 Description du traitement de la présente annexe ;
- Garantir que les traitements en cause répondent aux exigences de la réglementation, notamment que les Données à caractère personnel sont traitées de manière licite, loyale et transparente, qu'elles ont été collectées pour des finalités déterminées, explicites et légitimes et que l'information requise aux personnes concernées par le traitement a bien été fournie au moment de la collecte desdites données ;
- Documenter par écrit toute instruction et directive envers le Sous-traitant concernant le traitement des données par le Sous-traitant dans un document spécifique annexé aux présentes ;

- Veiller au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen de la part du Sous-traitant ;
- Superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.

7. Non-respect des obligations du sous-traitant

Le sous-traitant sera tenu responsable, en toutes circonstances, de tout dommage résultant d'un manquement à ses obligations ou de défaut de conformité à la Réglementation applicable en matière de protection des données personnelles.

A ce titre, le responsable de traitement ne pourra en aucun cas être tenu responsable d'une quelconque violation de Données personnelles traitées par le sous-traitant dans le cadre du traitement, si cette violation résulte d'un manquement du sous-traitant à l'une quelconque de ses obligations au titre de la réglementation applicable en matière de protection des données personnelles.

Le sous-traitant s'engage à indemniser le responsable de traitement (et respectivement chacun de ses dirigeants, employés et/ou agents) pour tout dommage résultant d'un manquement de sa part ou de ses Sous-traitants ultérieurs.

A ce titre, le sous-traitant garantit le responsable de traitement contre toute action, de quelque nature qu'elle soit, pouvant être intentée contre lui par une personne concernée ou encore tout tiers ou Autorité de contrôle, pour non-respect de la Réglementation applicable en matière de protection des données personnelles. En outre, le sous-traitant s'engage à indemniser le responsable de traitement et fera son affaire de tous frais supportés par ce dernier pour défendre ses droits ainsi que tous dommages-intérêts ou condamnation dont le responsable de traitement pourrait faire l'objet au titre de la violation de l'une de ses obligations et/ou de la Réglementation applicable en matière de protection des données personnelles.

La responsabilité du sous-traitant pourra également être engagée sur la base des dispositions des articles 226-16 et suivants du code pénal.