

MARCHE PUBLIC DE SERVICES

PREFECTURE DES YVELINES

SECRETARIAT GENERAL COMMUN DEPARTEMENTAL DES YVELINES

**Service de livraison de repas,
pour partie subventionnés par l'employeur,
à destination d'agents du ministère de l'Intérieur
exerçant dans les Yvelines
et intervenant au sein de neuf services répartis sur sept sites**

N° de marché	AS2-PROG0216-2025
--------------	-------------------

Clauses contractuelles de sous-traitance

Sommaire

I. Présentation des parties	2
II. Objet	2
III. Description du traitement faisant l'objet de la sous-traitance	2
IV. Durée du contrat	3
V. Obligations du sous-traitant vis-à-vis du responsable de traitement	3
VI. Sous-traitance	4
VII. Droit d'information des personnes concernées	4
VIII. Exercice des droits des personnes	5
IX. Notification des violations de données à caractère personnel	5
X. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations	6
XI. Mesures de sécurité	6
XII. Sort des données	7
XIII. Délégué à la protection des données	7
XIV. Registre des catégories d'activités de traitement	7
XV. Documentation	8
XVI. Obligations du responsable de traitement vis-à-vis du sous-traitant	8

I. Présentation des parties

Le Secrétariat Général Commun Département des Yvelines
Service action sociale
1 rue Jean Houdon
78000 Versailles
et représentée par le Préfet des Yvelines, Monsieur Frédéric ROSE

le responsable de traitements d'une part et

La société
située
.....
et représentée par
Délégué à la protection des données : (Facultatif)

le sous-traitant d'autre part,

II. 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 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 (*le règlement européen sur la protection des données*) et la loi informatique et liberté.

III. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le service suivant :

- Service de livraison de repas à destination des agents.

Ce service comprend la collecte et le traitement des données personnelles des agents dans le but de leur permettre de commander et payer des repas par le biais d'un portail de commande en ligne.

Les données à caractère personnel traitées sont notamment :

- Le nom,
- Le prénom,
- Le numéro de téléphone,
- Les numéros de carte bancaire,
- Les courriels,
- La signature,

Les finalités du traitement par le prestataire à l'occasion de cette prestation de service sont les suivantes :

- créer un accès en ligne au portail de commande
- traiter les commandes et livraison de repas
- suivre la facturation

Les catégories de personnes concernées sont les personnes physiques, dont les données personnelles seront traitées par le seul titulaire afin d'exécuter ses prestations.

IV. Durée du contrat

Le présent contrat est applicable à compter de la date de notification de l'accord-cadre pour la durée de la relation contractuelle entre le et le sous-traitant.

Durant cette période, le sous-traitant met en place tous les moyens aptes à assurer la confidentialité et la sécurité des données personnelles recueillies de manière à empêcher leur endommagement, effacement ou accès par des tiers non autorisés.

V. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données uniquement pour les seules finalités qui font l'objet de la sous-traitance et sur instructions du Secrétariat Général commun des Yvelines.

2. traiter les données conformément aux instructions documentées du responsable de traitement figurant en annexe du présent contrat. 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 États 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'État 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.

3. garantir la confidentialité des données à caractère personnel traitées dans le cadre des missions dévolues au maître d'œuvre et prévues au présent contrat.

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

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

5. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

VI. Sous-traitance

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement 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. Le responsable de traitement dispose d'un délai minimum de 10 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial 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 du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

VII. Droit d'information des personnes concernées

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

VIII. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider 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, de rectification, d'effacement et d'opposition, 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).

Pour ce faire, le sous-traitant informe les personnes concernées par les opérations de traitement que l'exercice du droit de rectification ou à l'effacement est exercé auprès du responsable de traitement par mél à l'adresse sgc-sdas-restauration@yvelines.gouv.fr

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 au DPO de la collectivité par courrier électronique à l'adresse suivante : sgc-sdas-restauration@yvelines.gouv.fr

Le sous-traitant doit répondre dans un délai de 15 jours.

IX. 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 24 heures après en avoir pris connaissance et par les moyens suivants : appel téléphonique pendant les horaires d'ouverture au 01 39 49 72 30, envoi d'un courrier électronique à l'adresse sgc-sdas-restauration@yvelines.gouv.fr, et envoi d'un courrier recommandé à l'attention de la Cheffe du service action sociale au 1 rue Jean Houdon 78010 Versailles Cedex.

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.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que 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.

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.

X. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

XI. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

1. toutes les personnes manipulant des données personnelles ont été formées sur le règlement n° 2016/679, dit règlement général sur la protection des données (RGPD) et ont signé un engagement de confidentialité pour les données personnelles manipulées ;
2. un identifiant unique est attribué à chaque utilisateur ;
3. une politique de mot de passe conforme aux recommandations de la CNIL est appliquée ;
4. les comptes sont automatiquement verrouillés après 5 saisies incorrectes du mot de passe ;
5. les permissions d'accès obsolètes sont supprimées tous les mois ;
6. réalisation tous les trimestres d'une revue des permissions et habilitations ;
7. les sessions des utilisateurs sont verrouillées automatiquement après 15 minutes d'inactivité ;
8. les données sont sauvegardées sur bande magnétique à minima une fois par semaine ;
9. les bandes magnétiques sont stockées dans un bâtiment différent de celui où sont les serveurs et dans une armoire verrouillée et ignifugée ;
10. les sauvegardes obsolètes sont détruites de manière sécurisée ;
11. les données au repos sont encryptées ;
12. un pare-feu protège chaque serveur et le réseau de production ;
13. les flux réseaux sur le réseau de production sont limités au strict minimum ;
14. tous les flux de données sont sécurisées et encryptés ;
15. toutes les mises à jour de sécurité sont installées sans délai sur tout le matériel présent sur le réseau de production ;
16. les portes des locaux contenant le matériel de production sont verrouillées en permanence ;
17. limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées ;
18. limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par le CNIL sur son site web.

XII. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage, au choix des parties,

- à détruire toutes les données à caractère personnel
- à renvoyer toutes les données à caractère personnel au responsable de traitement
- ou à renvoyer les données à caractère personnel 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.

XIII. Délégué à la protection des données

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

XIV. 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, selon les besoins ;
- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

XV. Documentation

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

XVI. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. fournir au sous-traitant les données visées au III des présentes clauses,
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant,
3. 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 sous-traitant,
4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

☐ Je certifie avoir recueilli le consentement de toutes les personnes dont les données personnelles seront traitées et conservées¹.

Validation du prestataire

le :

Signature :

¹ Cocher la case