

ANNEXE 3 AU CCAP : Application du Règlement Européen sur la Protection des Données 2016/679 du Parlement européen et du Conseil du 27 avril 2016

1. Désignation

Selon la terminologie utilisée par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 :

- Le responsable de traitement : L'organisme acheteur
- Le sous-traitant : Le titulaire du marché
- Le sous-traitant ultérieur : Le sous-traitant du titulaire

2. Objet

Les présentes dispositions 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, (ci-après, « **le règlement européen sur la protection des données** »RGPD).

3. 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 ou les service(s) suivant(s) : **MAPA N°25.672.01 - FOURNITURE ET LIVRAISON DE VETEMENTS DE TRAVAIL ET ACCESSOIRES DE PROTECTION POUR LES AGENTS DE LA CAISSE PRIMAIRE CENTRALE D'ASSURANCE MALADIE DES BOUCHES-DU-RHÔNE** La nature des opérations réalisées sur les données est susceptible de consister en: *la collecte, l'enregistrement, l'organisation, la structuration, la conservation, la modification, l'extraction, la consultation, l'utilisation, la diffusion, l'interconnexion, l'effacement, etc.*

Les données à caractère personnel traitées peuvent être des : *Données d'identification, données de contact, données personnelles, données professionnelles, données économiques et financières, données de connexion, données de localisation, données sensibles, etc.*

Les catégories de personnes concernées sont : des salariés et autre personnes susceptibles d'être concernées par le présent contrat.

Pour l'exécution des services ou travaux objet du présent contrat, le responsable de traitement peut être amené à mettre à la disposition du sous-traitant les informations nécessaires suivantes : *Nom, prénoms, date de naissance, sexe, tel, mail, adresse, identifiants de connexion, etc.*

4. Durée de conservation des données

Les données sont conservées pendant la durée du marché.

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

Le sous-traitant s'engage à :

5.1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/ont l'objet de la sous-traitance

5.2. 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 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

5.3. garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat

5.4. 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

5.5. 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**

5.6. 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 8 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.

5.7. 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.

5.8. 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).

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 24 heures après en avoir pris connaissance et par courrier électronique dont l'adresse sera transmise sous-traitant dès la notification du contrat.

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.

5.10. 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.

5.11. Mesures de sécurité

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

- 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 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.

En outre, le sous-traitant s'engage à la demande du responsable de traitement des données à communiquer la Politique de Sécurité Informatique mise en œuvre dans l'entreprise, la localisation de ses infrastructures de stockage des données, ainsi que tout autre élément de nature à permettre au responsable de traitement des données de s'assurer que le sous-traitant présentent des 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 et garantisse la protection des droits des personnes concernées.

5.12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à la demande du responsable de traitement des données :

- à détruire toutes les données à caractère personnel ou
- 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.

5.13. 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.

5.14. 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 :
 - o la pseudonymisation et le chiffrement des données à caractère personnel;
 - o des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
 - o 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;
 - o une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

5.15. 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.

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

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données visées au 3.3 des présentes dispositions ;
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
- 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 ;

- superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

7. Responsabilité – dommages et intérêts en cas de non-respect des dispositions liées à la conformité au RGPD

Le responsable de traitement des données se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par le sous-traitant.

En cas de non-respect par le sous-traitant de ses engagements, le responsable de traitement des données se réserve le droit de résilier le marché dans les conditions prévues à l'article 15 du CCP, sans indemnité en faveur du sous-traitant, au jour de la réception par ce dernier de la lettre recommandée avec accusé de réception portant résiliation et cela sans préjudice des dommages et intérêts qui pourront lui être réclamés.

Enfin il est rappelé qu'en cas de non-respect des dispositions précitées, la responsabilité du sous-traitant peut également être engagée sur la base des dispositions des articles 226-17 et 226-5 du code pénal.