Annexe :

Conformité au règlement européen

sur la protection des données personnelles

SOMMAIRE

1 CONFORMITE AU RGPD **ERREUR ! SIGNET NON DEFINI.**

1.1 OBJET 3

1.2 DEFINITIONS 3

1.3 DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DU MARCHE 4

1.4 DUREE 4

1.5 OBLIGATIONS DES PARTIES 4

1.5.1 Obligations du sous-traitant vis-à-vis du responsable de traitement 4

1.5.2 Obligations du responsable de traitement vis-à-vis du Sous-traitant 5

1.6 INTERVENANTN DU SOUS-TRAITANT 5

1.7 DROIT D'INFORMATION DES PERSONNES CONCERNEES 6

1.8 EXERCICE DES DROITS DES PERSONNES 6

1.9 NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL 6

1.10 CONSEIL DU SOUS-TRAITANT DANS LE CADRE DU RESPECT PAR LE RESPONSABLE DE TRAITEMENT DE SES OBLIGATIONS 7

1.11 MESURES DE SECURITE 7

1.12 AUDIT 7

1.13 SORT DES DONNEES 8

1.14 DELEGUE A LA PROTECTION DES DONNEES 9

1.15 REGISTRE DES CATEGORIES D'ACTIVITES DE TRAITEMENT 9

1.16 SANCTIONS ENCOURUES EN CAS DE NON-RESPECT 9

1.17 TRAITEMENT DE DONNEES DITES SENSIBLES 10

Les exigences de conformité RGPD décrites ci-dessous s'appliquent à l'ensemble de la prestation objet du marché.

Le non-respect des exigences de conformité RGPD définies par la suite fait l'objet de pénalités au titre des obligations prévus au règlement européen sur la protection des données personnelles (Règlement UE 2016/679 du 27 avril 2016) entré en vigueur le 25 mai 2018 et la loi Informatique et Libertés (Loi 78-17 du 6 janvier 1978 modifiée).

1.1 OBJET

Les présentes dispositions ont pour objet de définir les conditions dans lesquelles le titulaire du marché, en tant que Sous-traitant au sens de la règlementation relative à la protection des données personnelles, s'engage à effectuer pour le compte du pouvoir adjudicateur, Responsable de traitement, les opérations de traitement de données à caractère personnel définies ci-après dans le cadre des prestations prévues au titre du marché.

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*** »).

1.2 DEFINITIONS

« **Traitement de données** » désigne « toute opération, ou tout ensemble d'opérations [...] appliquées à des données[...], telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction » (RGPD, Chapitre I, art. 4-2),

« **Responsable de traitement** » désigne celui « qui détermine les finalités et les moyens du traitement » (RGPD, Chapitre I, art. 4-7). Au sens du code de la commande publique, il s'agit du pouvoir adjudicateur (Article L. 1211-1 de l'Ordonnance n° 2018-1074 du 26 novembre 2018 portant partie législative du code de la commande publique),

« Sous-traitant » (au sens du RGPD) désigne celui qui traite des données personnelles pour le compte, sur instruction et sous l'autorité du responsable de traitement. Le sous-traitant est l'opérateur économique qui conclut le marché avec le pouvoir adjudicateur,

« **Intervenant du sous-traitant** » désigne un intervenant que le sous-traitant a recruté après avoir obtenu l'autorisation écrite du responsable de traitement. Cette demande d'autorisation se matérialise par remise d'un DC4.

1.3 DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DU MARCHE

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 : **Prestations de médecine préventive et de santé au travail au bénéfice des agents du Cned, du Réseau Canopé et de l'ONISEP**

La nature des opérations réalisées sur les données est la suivante : **Suivi informatique de gestion des dossiers médicaux**

La ou les finalité(s) du traitement est/sont la/les suivante(s) : **Soins du patient dans le cadre de la médecine du travail**

Les données à caractère personnel traitées sont les suivante(s) : **Nom, prénoms, sexe, nationalité, date de naissance, lieu de naissance, taille, adresse, âge, poids, suivi médical (antécédents médicaux, données génétiques, maladies, prestations de soins réalisés, résultats d'examens notamment biologiques, traitements, handicap, etc.)**

Les personnes concernées par ces traitements sont les suivantes : **Agents du Cned, du réseau Canopé et de l'ONISEP**

Pour l'exécution du service objet du présent marché, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes : **Dossier administratif de l'agent concerné**

1.4 DUREE

Les présentes dispositions sont valables pour toute la durée du marché.

1.5 OBLIGATIONS DES PARTIES

1.5.1 OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

Le Sous-traitant s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du marché ;
- 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 de traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :
    - 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.
- 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.

1.5.2 OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le Responsable de traitement s'engage à :

- fournir au sous-traitant les données visées à l'article 1 de la présente annexe ;
- 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.

1.6 INTERVENANT DU SOUS-TRAITANT

Le Sous-traitant peut faire appel à un Intervenant (ci-après, « l'Intervenant ») 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 Intervenants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées de l'Intervenant et les dates du contrat de sous-traitance. Le Responsable de traitement dispose d'un délai maximum vingt-et-un (21) jours ouvrables à compter de la date de réception de cette information pour présenter ses objections. Le silence du Responsable de traitement gardé pendant ces vingt-et-un jours vaut également acceptation de l'Intervenant et agrément des conditions de paiement conformément à l'article R2193-4 du Code de la Commande Publique.

L'Intervenant du Sous-traitant est tenu de respecter les obligations du présent marché pour le compte et selon les instructions du Responsable de Traitement. Il appartient au Sous-traitant de s'assurer que l'Intervenant 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 l'Intervenant ne remplit pas ses obligations en matière de protection des données, le Sous-traitant demeure pleinement responsable devant le Responsable de traitement de l'exécution par l'Intervenant de ses obligations.

1.7 DROIT D'INFORMATION DES PERSONNES CONCERNEES

Il appartient au Responsable de traitement de fournir, au moment de la collecte des données, aux personnes concernées par les opérations de traitement de leurs données à caractère personnel, l'information relative aux traitements de données qu'il réalise.

1.8 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 par la collecte et le traitement de leurs données à caractère personnel : 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).

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 l'adresse suivante : dpo@ac-cned.fr**.**

1.9 NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

Le Sous-traitant notifie au Responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 36 (trente-six) heures après en avoir pris connaissance et par le moyen suivant : mail aux adresses suivantes : dpo@ac-cned.fr et rssi@ac-cned.fr, même si la violation en question n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Cette notification est accompagnée de toute documentation utile (voir la liste ci-dessous) afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Le Responsable de traitement notifie à l'autorité de contrôle compétente, les violations de données à caractère personnel dans les meilleurs délais et 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.

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 de personnes concernées par la violation et les catégories et le nombre 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 (Sur les données et les droits et libertés des personnes concernées);

• 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.

Le cas échéant, le Responsable de traitement communique 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.

1.10 CONSEIL DU SOUS-TRAITANT DANS LE CADRE DU RESPECT PAR LE RESPONSABLE DE TRAITEMENT DE SES OBLIGATIONS

Le Sous-traitant conseille 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.

1.11 MESURES DE SECURITE

Le Sous-Traitant s'engage à mettre en œuvre les mesures de sécurité conformes à l'état de l'art et notamment les mesures suivantes:

- 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 tout état de cause, le Sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par Référentiel Général de Sécurité (RGS).

1.12 AUDIT

Le Sous-traitant met à la disposition du Responsable de traitement, par courriel et à la demande de celui-ci, tout document nécessaire permettant de démontrer le respect de ses obligations en qualité de Sous-traitant au titre du marché. Tout autre mode de transmission de ces documents s'effectue aux frais du Responsable de traitement.

Le Responsable de traitement peut réclamer auprès du Sous-traitant des explications complémentaires si les documents fournis ne lui permettent pas de vérifier le respect de ses obligations. Le Responsable de traitement formule alors une demande écrite auprès du Sous-traitant, par lettre recommandée avec accusé de réception, dans laquelle il justifie et documente sa demande d'explication complémentaire. Le Sous-traitant s'engage à apporter une réponse au Responsable de traitement dans les meilleurs délais.

Si malgré la réponse du Sous-traitant, le Responsable de traitement remet en cause la véracité ou la complétude des informations transmises ou en cas de risques imminents à la sécurité des Données Personnelles, ce dernier peut procéder à un audit sur site sous réserve du respect des conditions suivantes :

1 - Le Responsable de traitement formule une demande écrite d'audit sur site auprès du Sous-traitant, par lettre recommandée avec accusé de réception, en justifiant et en documentant sa demande ;

2 - Le Sous-traitant s'engage à apporter une réponse au Responsable de traitement en précisant le périmètre et les conditions de réalisation de l'audit sur site. La sécurité du système d'information du Sous-traitant reposant sur leur accès restreint, le périmètre d'un audit sur site est limité aux processus du Sous-traitant permettant de réaliser le Service et/ou les prestations, en qualité de Sous-traitant du ou des traitements de Données Personnelles confié(s) par le Responsable de traitement. La durée de l'audit ne doit pas dépasser deux (2) jours ouvrés qui sont facturés par le Sous-traitant au Responsable de traitement selon le tarif des prestations en vigueur au moment du déroulement de l'audit ;

3 - Cette mission d'audit peut être réalisée par les auditeurs internes du Responsable de traitement ou peut être confiée à tout prestataire au choix du Responsable de traitement, non concurrent du Sous-traitant ;

4 - Les auditeurs doivent prendre un engagement formel de non-divulgation des informations recueillies chez le Sous-traitant quel qu'en soit le mode d'acquisition. La signature de l'accord de confidentialité par les auditeurs doit être préalable à l'audit et communiquée au Sous-traitant.

Dans le cadre de l'audit, le Sous-traitant donne accès à ses locaux, et d'une manière générale aux documents et aux personnes nécessaires afin que les auditeurs puissent conduire l'audit dans des conditions satisfaisantes. Il est entendu que cet audit ne doit pas avoir pour conséquence de perturber l'exploitation du Service et/ou la réalisation des prestations.

Le rapport d'audit est mis à la disposition du Sous-traitant par les auditeurs avant d'être finalisé, de telle sorte que le Sous-traitant puisse formuler toutes ses observations, le rapport final devant tenir compte et répondre à ces observations. Le rapport d'audit est ensuite adressé au Sous-traitant et fait l'objet d'un examen dans le cadre d'une réunion entre les parties.

Au cas où le rapport d'audit final révèlerait des manquements aux engagements pris au titre de l'exécution du Service et/ou des prestations, le Sous-traitant doit proposer un plan d'actions correctives dans un délai de vingt (20) jours ouvrés maximum à compter de la réunion entre les parties.

Sauf changement de circonstance et événement légitimant la mise en œuvre d'un audit dans un délai plus court, les audits ne peuvent être réalisés par le Responsable de traitement sur site du Sous-traitant, qu'une fois pendant la période initiale du marché, puis une fois par période de reconduction.

1.13 SORT DES DONNEES

Au terme de la prestation de services relatifs au traitement de ces données, le Sous-traitant s'engage à renvoyer l'intégralité des données personnelles qui lui a été confiée 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, après s'être assuré auprès du Responsable de traitement que ce dernier dispose bien de ces informations.

1.14 DELEGUE A LA PROTECTION DES DONNEES

Le Sous-traitant informe le Responsable de traitement des coordonnées de son délégué à la protection des données par courriel à l'adresse dpo@ac-cned.fr.

1.15 REGISTRE DES CATEGORIES D'ACTIVITES 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 de 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 ;
    - 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.

1.16 SANCTIONS ENCOURUES EN CAS DE NON-RESPECT

Il est aussi rappelé au Sous-traitant que la violation des dispositions du règlement européen 2016/679 du 27 avril 2016, expose celui-ci :

- aux sanctions pénales prévues aux articles 226-16 à 226-24 du code pénal (conformément au chapitre VIII de la loi n°78-17 modifiée) ;
- aux sanctions prévues aux articles 82 et 83 du Règlement européen 2016/679 du 27 avril 2016, à compter du 25 mai 2018 (allant jusqu'à 20 millions d'euros d'amende ou jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent).

En cas de manquement de transmission des demandes des droits des personnes, le Sous-traitant s’engage à réparer tout préjudice subi par les demandeurs.

1.17 TRAITEMENT DE DONNEES DITES SENSIBLES

Dans le cas d'un traitement de données à caractère personnel ou d'un traitement de données dites sensibles, l'application du RGPD et de la loi informatique et libertés exigent des obligations particulières indiquées à l’article 5.1.5 du CCTP.