***Annexe n°2 encadrant les traitements de données à caractère personnel (version du 13/05/25)***

***I. Objet***

*Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Titulaire effectue pour le compte du CEA 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 (ci-après, «****le règlement européen sur la protection des données****»).*
* *La décision d’exécution (UE) 2021/915 de la Commission européenne en date du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l’article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l’article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil.*

***II. Description du traitement faisant l’objet du transfert des données à caractère personnel***

*Le Titulaire est autorisé à traiter pour le compte du CEA les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :*

|  |
| --- |
| *Description des opérations réalisées sur les données[[1]](#footnote-1) :*   * ***Utilisation des données des salariés via l’application nationale HYGIEKOS dans le cadre des convocations médicales du Service de Santé au Travail*** * ***Tri des résultats d’analyses et dispatching aux médecins*** * ***Gestion des dossiers pour les visites médicales*** * ***Rédaction de courrier à vocation médicale à la demande des médecins*** |
| *Finalité(s) du traitement[[2]](#footnote-2) :* ***Gestion des convocations médicales et dossiers médicaux des salariés*** |
| *Type de données à caractère personnel traitées[[3]](#footnote-3) :*  ***Données administratives des salariés (Nom, Prénom, date de naissance, téléphone, adresse mail) et données de santé.*** |
| *Catégories de personnes concernées[[4]](#footnote-4) :*  ***Salariés CEA, Salariés Entreprises Extérieurs, Partenaires, stagiaires, intérimaires, CDD, Candidats à l’embauche.*** |
| *Autres précisions ou interdictions[[5]](#footnote-5) :* ***Les données ne sont que sur le système d’information CEA*** |

***III. Obligations du Titulaire vis-à-vis du CEA***

*Le Titulaire s'engage à :*

1. *Traiter les données****uniquement pour la ou les seule(s) finalité(s)****qui fait/font l’objet de la prestation ;*
2. *Traiter les données****conformément aux instructions documentées****du CEA. Si le Titulaire 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 CEA. En outre, si le Titulaire 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 CEA 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 du présent marché ;*
4. *Veiller à ce que les****personnes autorisées à traiter les données à caractère personnel****en vertu du présent marché :*
5. *S’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,*
6. *Reçoivent la formation nécessaire en matière de protection des données à caractère personnel*
7. *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***
8. *Aider le CEA à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le Titulaire :* 
   1. *L’obligation de procéder à une évaluation de l’incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d’impact relative à la protection des données ») lorsqu’un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;*
   2. *L’obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le CEA ne prenait pas de mesures pour atténuer le risque;*
   3. *L’obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le CEA si le Titulaire apprend que les données à caractère personnel qu’il traite sont inexactes ou sont devenues obsolètes;*
   4. *Les obligations prévues à l’article 32 du règlement européen sur la protection des données.*
9. ***Données sensibles***

*Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le Titulaire applique des limitations spécifiques et/ou des garanties supplémentaires.*

1. ***Sous-traitance ultérieure***

*Le Titulaire informe spécifiquement par écrit le CEA de toute sous-traitance dans le cadre du marché au moins 1 mois à l’avance, donnant ainsi au CEA suffisamment de temps pour pouvoir s’opposer au choix des sous-traitants ultérieurs. Le Titulaire fournit au CEA les informations nécessaires pour lui permettre d’exercer son droit d’opposition (nom, adresse, nom/fonction et coordonnées de la personne de contact, description du traitement confié au sous-traitant (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés).*

*Lorsque le Titulaire sous-traite pour mener des activités de traitement spécifiques (pour le compte du CEA), il le fait au moyen d’un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au Titulaire en vertu des présentes clauses. Le Titulaire veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement européen sur la protection des données.*

*À la demande du CEA, le Titulaire lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d’affaires ou d’autres informations confidentielles, y compris les données à caractère personnel, le Titulaire peut expurger le texte du contrat avant d’en diffuser une copie.*

*Le Titulaire demeure pleinement responsable, à l’égard du CEA, de l’exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le Titulaire informe le CEA de tout manquement du sous-traitant ultérieur à ses obligations contractuelles. Le Titulaire convient avec le sous-traitant ultérieur d’une clause du tiers bénéficiaire selon laquelle, dans le cas où le Titulaire a matériellement disparu, a cessé d’exister en droit ou est devenu insolvable, le CEA a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d’effacer ou de renvoyer les données à caractère personnel.*

***9. Transferts internationaux***

1. *Tout transfert de données vers un pays tiers ou une organisation internationale par le Titulaire n’est effectué que sur la base d’instructions documentées du CEA ou afin de satisfaire à une exigence spécifique du droit de l’Union ou du droit de l’État membre à laquelle le sous-traitant est soumis et s’effectue conformément au chapitre V du règlement européen sur la protection des données.*
2. *Le CEA convient que lorsque le Titulaire recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du CEA) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement européen sur la protection des données, le Titulaire et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement européen sur la protection des données en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l’article 46, paragraphe 2, du règlement (UE) 2016/679 le 4 juin 2021 dans une décision d’exécution (UE) 2021/914, pour autant que les conditions d’utilisation de ces clauses contractuelles types soient remplies.* 
   1. ***Droit d’information des personnes concernées***

*Le Titulaire, au moment de la collecte des données, doit fournir aux personnes concernées l’information relative aux traitements de données qu’il réalise. La formulation et le format de l’information doit être convenue avec le CEA avant la collecte de données.*

* 1. ***Exercice des droits des personnes***

*Dans la mesure du possible, le Titulaire doit aider le CEA 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).*

*Le Titulaire doit répondre, au nom et pour le compte du CEA et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d’exercice de leurs droits, s’agissant des données faisant l’objet de la prestation prévue par le présent marché.*

* 1. ***Notification des violations de données à caractère personnel***

*Le Titulaire notifie au CEA toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance en adressant un email avec accusé de réception à : dpd@cea.fr. Cette notification est accompagnée de toute documentation utile afin de permettre au CEA, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.*

* ***Violation de données en rapport avec des données traitées par le CEA***

*En cas de violation de données à caractère personnel en rapport avec des données traitées par le CEA, le Titulaire prête assistance au CEA:*

1. *Aux fins de la notification de la violation de données à caractère personnel à l’autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le CEA en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques);*
2. *Aux fins de l’obtention des informations suivantes qui, conformément à l’article 33, paragraphe 3, du règlement européen sur la protection des données, doivent figurer dans la notification du CEA, et inclure, au moins:*
3. *La nature des 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;*
4. *Les conséquences probables de la violation de données à caractère personnel;*
5. *Les mesures prises ou les mesures que le CEA 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.*

*Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais;*

1. *Aux fins de la satisfaction, conformément à l’article 34 du règlement européen sur la protection des données, de l’obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes physiques.*

* ***Violation de données en rapport avec des données traitées par le Titulaire***

*En cas de violation de données en rapport avec des données traitées par le Titulaire, la notification faite au CEA contient au moins:*

1. *Une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés);*
2. *Les coordonnées d’un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel;*
3. *Ses conséquences probables et les mesures prises ou les mesures qu’il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.*

*Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.*

* 1. ***Mesures de sécurité***

*Le Titulaire s’engage à mettre en œuvre les mesures de sécurité suivantes :*

|  |  |
| --- | --- |
| *Pseudonymisation des données à caractère personnel (si applicable)* | ***Sans Objet*** |
| *Chiffrement des données à caractère personnel* | ***Sans Objet*** |
| *Moyens permettant de garantir la confidentialité et l’intégrité des données* | ***Données gérées sur système d’information interne médical. Les traitements sont réalisés en cohérence avec la PSSI CEA.*** |
| *Moyens permettant de rétablir la disponibilité des données et leur accès dans des délais appropriés en cas d’incident physique ou technique* | ***En cohérence avec PSSI*** |
| *Procédure visant à tester, analyser, évaluer l’efficacité des mesures de sécurité* | ***Sans Objet*** |

* 1. ***Sort des données***

*Au terme du marché, le Titulaire s’engage à renvoyer toutes les données à caractère personnel au CEA sauf instruction différente reçue du CEA. Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du Titulaire. Une fois détruites, le Titulaire doit justifier par écrit de la destruction.*

* 1. ***Délégué à la protection des données***

*Le Titulaire communique au CEA****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.*

* 1. ***Registre des catégories d’activités de traitement***

*Le Titulaire déclare****tenir par écrit un registre****de toutes les catégories d’activités de traitement effectuées pour le compte du CEA comprenant les éléments imposés par le règlement européen sur la protection des données.*

* 1. ***Documentation***

*Le Titulaire met à la disposition du CEA****la documentation nécessaire pour démontrer le respect de toutes ses obligations****et pour permettre la réalisation d'audits, y compris des inspections, par le CEA ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.*

***IV. Obligations du CEA vis-à-vis du Titulaire***

*Le CEA s’engage à :*

1. *Fournir au Titulaire les données visées au II des présentes clauses ;*
2. *Documenter par écrit toute instruction concernant le traitement des données par le Titulaire ;*
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 Titulaire ;*
4. *Superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire.*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Préciser ce que le prestataire va faire avec les données. Par exemple, pour une prestation d’infogérance : intervention sur les systèmes d’information, maintenance… [↑](#footnote-ref-1)
2. Raison pour laquelle les données sont traitées. Par exemple, infogérance, réservation de voyages, gestion des inscriptions à une conférence, organisation et suivi des élections professionnelles … [↑](#footnote-ref-2)
3. Les types de données sont principalement : Etat civil, Vie personnelle, Vie professionnelle, Informations économiques et financières, Données de connexion, N° de sécu, Données biométriques, Données génétiques, Difficultés sociales, Données de santé... [↑](#footnote-ref-3)
4. Les catégories de personnes sont principalement : Salariés CEA, Salariés d'entreprises extérieures sur site CEA / intérimaires, Stagiaires, Clients, Fournisseurs, Visiteurs, Sujets de recherche, Grand public... [↑](#footnote-ref-4)
5. Préciser, par exemple, si les données ne sont accessibles que sur site CEA. [↑](#footnote-ref-5)