

Annexe n°2 au projet de marché n°B25-01268-FL

Traitements de données à caractère personnel

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Titulaire effectue des opérations de traitement de données à caractère personnel sur instructions documentées du CEA.

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 sur instruction documentée du CEA les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) (à renseigner par le CEA –prescripteur) :

Description des opérations réalisées sur les données : Paramétrage des plats et des menus, Paiement des convives
Finalité(s) du traitement : Gestion de la restauration Le log/clef de caisse SAGERE est un logiciel de gestion de la restauration qui permet dans tous les selfs CEA: <ul style="list-style-type: none">• Le paramétrage des plats et des menus• Le paramétrage de la part patronale• Le paramétrage de la quote-part des sociétés hébergées• Le paiement des convives Le logiciel SAGERE est composé : <ul style="list-style-type: none">• D'un serveur centralisé à Saclay• De caisses (107 caisses)• De postes de gestion (1 ou 2 postes de gestion par centre permettant les opérations de caisses mais également le paramétrage des menus, la quote-part employeur...).
Type de données à caractère personnel traitées : Etat civil (nom, prénom, matricule), vie personnelle (menus), vie professionnelle (unité, projets, temps de travail, société employeur), informations d'ordre économique et financier (coordonnées bancaires en cas de post-paiement), Données de connexion
Catégories de personnes concernées : Toute personne sur centre CEA prenant ses repas dans le restaurant d'entreprise (salariés, personne non salariée ayant un compte de restauration...)
Autres précisions ou interdictions :

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. Ne pas croiser les données recueillies avec d'autres données permettant d'établir une corrélation religieuse ou de santé ;
3. 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 ;
4. **garantir la confidentialité** des données à caractère personnel traitées dans le cadre du présent marché ;
5. 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
6. 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**
7. Aider le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant:
 - a. 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;
 - b. 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 responsable du traitement ne prenait pas de mesures pour atténuer le risque;
 - c. L'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes;
 - d. Les obligations prévues à l'article 32 du règlement (UE) 2016/679.

8. 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 sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

9. Sous-traitance ultérieure

Le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue, et pour les activités suivantes : restauration.

Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de

modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins un mois à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), 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 sous-traitant en vertu des présentes clauses. Le sous-traitant 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 (UE) 2016/679 et/ou du règlement (UE) 2018/1725

À la demande du responsable du traitement, le sous-traitant 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 sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.

Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire. Dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, le responsable du traitement 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.

Liste des sous-traitants ultérieurs : Les sous-traitants seront déclarés à l'obtention ou en cours d'exécution du marché.

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants:

Sous-traitant 1 :

- *Nom : ...*
- *Adresse : ...*
- *Nom, fonction et coordonnées de la personne de contact : ...*
- *Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés): ...*

Sous-traitant 2 : ...

10. Transferts internationaux : pas de transfert à l'international dans le cadre de ce contrat.

a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement 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 (UE) 2016/679 ou du règlement (UE) 2018/1725.

b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 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.

EN CAS DE TRANSFERT HORS UE SE REFERER AUX MODULES 1 à 4 (annexe transferts hors UE).

11. 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.

12. 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.

13. 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 responsable du traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement:

- a) 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 responsable du traitement 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) ;
- b) Aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins:
 - 1) 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;
 - 2) Les conséquences probables de la violation de données à caractère personnel;
 - 3) Les mesures prises ou les mesures 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.

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 ;

- c) Aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, 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 sous-traitant

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

- a) 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);
- b) 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;
- c) 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.

14. Mesures de sécurité

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

Pseudonymisation des données à caractère personnel (si applicable) ⁶	N/A
Chiffrement des données à caractère personnel ⁷	Les données sont hébergées sur un réseau isolé distinct (« bulle SAGERE »). Elles ne sont pas chiffrées dans l'application. Les données extraites de SAGERE, dès lors qu'elles contiennent les données bancaires, doivent toujours être enregistrées dans un container chiffré (quel que soit le support : clé, disque dur...). Leur communication se fait systématiquement dans un container chiffré ou par un mail chiffré.

⁶ La « pseudonymisation » consiste à remplacer les noms/prénoms des personnes par un numéro d'identifiant. La pseudonymisation peut être obligatoire : par exemple, pour les traitements à des fins de recherche qui contiennent des données de santé ou des données génétiques.

⁷ A minima, il faut chiffrer les données lors de la transmission de données personnelles

Moyens permettant de garantir la confidentialité et l'intégrité des données	<p>Les postes de gestion SAGERE sont dans des locaux fermés à clé. Ces postes sont sécurisés avec un pare-feu et un anti-virus. Seules les personnes habilitées ont accès aux postes de gestion, par un identifiant et un mot de passe Windows puis SAGERE. Un verrouillage automatique de la session Windows est systématiquement mis en place.</p> <p>SAGERE contient un système de journalisation des données qui permet de savoir si des fiches ont été modifiées ou supprimées.</p> <p>Au sein de chaque restaurant, l'application SAGERE est accessible au niveau des caisses, pour permettre la saisie des menus pris par les convives. L'accès aux données n'est possible qu'avec le badge de la personne au moment de son passage en caisse ou en saisissant ses noms et prénoms après vérification de son identité.</p>
Moyens permettant de rétablir la disponibilité des données et leur accès dans des délais appropriés en cas d'incident physique ou technique	Les données de SAGERE font l'objet d'une sauvegarde journalière par le CEA qui permettent de les rétablir en cas de suppression ou modification non souhaitée.
Procédure visant à tester, analyser, évaluer l'efficacité des mesures de sécurité	Procédure décrite dans le Plan de Sécurité des Systèmes d'informations (PSSI) du CEA, le réseau Sagere étant sur le réseau CEA.

15. 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.

16. 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.

17. 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.

18. 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.

III. 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.