

Les Règles d'Entreprise Contraignantes de Sodexo

Politique en tant que
Sous-traitant



Table des matières

1. Introduction générale	5
Introduction	6
Qu'est-ce que le RGPD ?	7
Le RGPD impacte-t-il le flux transfrontalier des Données Personnelles au sein de Sodexo ?	8
Quel est la finalité et le champ d'application des BCR de Sodexo ?	8
En pratique, qu'est-ce que cela signifie pour les Données Personnelles collectées et utilisées en Europe ?	10
Rôles dans le cadre de la Protection des Données	11
Informations additionnelles	11
2. Les Règles	13
RÈGLE 1 - ÊTRE EN CONFORMITÉ AVEC LES BCR, LE RGPD ET LES RÉGLEMENTATIONS LOCALES APPLICABLES	14
RÈGLE 2 - GARANTIR LA LICÉITÉ, LA LOYAUTÉ ET LA TRANSPARENCE	15
RÈGLE 3 - GARANTIR UNE LIMITATION DES FINALITÉS	16
RÈGLE 4 - GARANTIR LA MINIMISATION DES DONNÉES	16
RÈGLE - 5 GARANTIR L'EXACTITUDE	17
RÈGLE 6 - GARANTIR LA LIMITATION DE LA CONSERVATION	17
RÈGLE 7 - PRENDRE LES MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES APPROPRIÉES	18
RÈGLE 8 - PROTÉGER L'UTILISATION DES DONNÉES PERSONNELLES SENSIBLES ET DES AUTRES CATÉGORIES PARTICULIÈRES DE DONNÉES PERSONNELLES....	20
RÈGLE 9 - CONSERVER LES REGISTRES DES ACTIVITÉS DE TRAITEMENT DES DONNÉES	20
RÈGLE 10 - RESPECTER LES DROITS DES PERSONNES CONCERNÉES.....	22
RÈGLE 11 - RESPECTER LES CONDITIONS RELATIVES AU PROFILAGE ET AUX PRISES DE DÉCISIONS INDIVIDUELLES ENTIÈREMENT AUTOMATISÉES ET METTRE EN ŒUVRE LES SAUVEGARDES APPROPRIÉES	22
RÈGLE 12 - TRANSPARENCE ET INFORMATIONS DE LA PERSONNE CONCERNÉE	23
RÈGLE 13 - ASSURER UNE PROTECTION ADÉQUATE POUR LE TRANSFERT TRANSFRONTALIERS DE DONNÉES PERSONNELLES.....	23
RÈGLE 14 - RESPECT DE LA PROTECTION DES DONNEES DÈS LA CONCEPTION ET PAR DÉFAUT	24
RÈGLE 15 - EFFECTUER UNE ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNÉES (AIPD)	24
RÈGLE 16 - FORMATION ET SENSIBILISATION	25
RÈGLE 17 - GERER LES DROITS RELATIFS A LA PROTECTION DES DONNÉES.....	26
RÈGLE 18 - ÉVALUER LA CONFORMITÉ : PROGRAMME D'AUDIT	27

RÈGLE 19 - SUIVRE L'APPLICATION DES BCR	28
RÈGLE 20 - ÉQUIPE DÉDIÉE À LA PROTECTION DES DONNÉES DU GROUPE ET RÉSEAU DE POINTS DE CONTACT LOCAUX	28
RÈGLE 21 - DROITS DES TIERS BÉNÉFICIAIRES	29
RÈGLE 22 - RESPONSABILITÉ	32
3. Dispositions finales.....	34
RÈGLE 23 - ACTIONS EN CAS DE REGLEMENTATIONS OU PRATIQUES NATIONALES EMPÊCHANT LE RESPECT DES BCR – DEMANDE JURIDIQUEMENT CONTRAIGNANTE DE COMMUNICATION DES DONNÉES PERSONNELLES	35
RÈGLE 24 - COOPÉRATION AVEC LES AUTORITÉS DE CONTRÔLE	38
RÈGLE 25 - ACTUALISATION DES BCR.....	39
RÈGLE 26 - CARACTERE CONTRAIGNANT DES BCR	40
4. Annexes	41
Annexe 1 - Définitions	43
Annexe 2 - Politique Globale de collecte et de conservation des données (Sous-traitant)..	46
Annexe 3 - Procédure de coopération des BCR	49
Annexe 4 - Procédure de mise à jour des BCR.....	50
Annexe 5 - Politique Globale relative à la protection des Données Personnelles de Sodexo	52
Annexe 6 - Politique Globale de gestion des droits des Personnes Concernées.....	53
Annexe 7 - Description du champ d'application matériel de la Politique en tant que Sous-traitant	54

Dans ce document, « Sodexo » désigne collectivement les entités Sodexo qui ont adhéré à la Politique en tant que Sous-traitant des Règles d'Entreprise Contraignantes (Binding Corporate Rules en anglais ou « BCR ») en signant un accord intra-groupe d'adhésion (« entité Sodexo » ou « entités Sodexo » ou « membres de la Politique en tant que Sous-traitant »)¹.

AUDIENCE CIBLE :

Tous les employés de Sodexo (y compris les nouveaux employés et toute personne agissant au nom et pour le compte de Sodexo, tels que les consultants et les prestataires individuels.

PUBLIÉ PAR :

La Direction Juridique du Groupe Sodexo (L'équipe dédiée à la Protection des Données du Groupe)

VERSION :

1.0

REMPLECE :

La Politique en tant que Sous-traitant des Règles d'Entreprise Contraignantes (« BCR ») de Sodexo remplace toutes les politiques et avis de Protection des Données de Sodexo qui existent à la date d'entrée en vigueur dans la mesure où elles [C1] traitent les mêmes questions et qu'elles ne sont pas conformes à cette politique. [C1]Normally should be "ils" here as avis is masculine. Please check with the client. I did not want to update his/her changes

DATE D'ENTRÉE EN VIGUEUR :

21 Décembre 2023

S'il y a des divergences entre la version anglaise de cette politique et une version traduite, la version anglaise prévaudra.

Droit d'auteur de Sodexo, tous droits réservés.

¹ Entité de Sodexo ou Entités de Sodexo désigne toute filiale du Groupe Sodexo (c'est-à-dire l'entité ou les entités contrôlées directement ou indirectement par ou sous contrôle commun avec Sodexo SA, telles que définies par l'article L. 233-3 du Code de commerce français) soumis aux Règles d'Entreprise Contraignantes de Sodexo.

01

Introduction générale



Introduction

Sodexo a établi un cadre et une déclaration claire sur le sujet de la protection des Données Personnelles dans le cadre du programme global de conformité à la Protection des Données de Sodexo, à savoir les Règles d'Entreprise Contraignantes de Sodexo (« BCR » ou « BCR de Sodexo »).

Les BCR de Sodexo sont intégrées dans le Code de Conduite - Principes d'intégrité de Sodexo. En vertu de ce code de conduite, les employés sont tous responsables et censés respecter et protéger la confidentialité et les informations confidentielles de leurs parties prenantes, notamment les candidats à un emploi, les employés, les clients, les consommateurs/bénéficiaires, les fournisseurs/vendeurs, les prestataires/sous-traitants, et autres tierces parties, conformément aux lois et aux réglementations applicables.

Les BCR se composent des deux politiques suivantes avec leurs annexes :

- La Politique en tant que Responsable du Traitement des Règles d'Entreprise Contraignantes en matière de Protection des Données (« Politique en tant que Responsable du Traitement » ou « BCR-RT ») ;
- La Politique en tant que Sous-traitant des Règles d'Entreprise Contraignantes en matière de Protection des Données (« Politique en tant que Sous-traitant » ou « BCR-ST »).

Les BCR de Sodexo ont été créées pour établir l'approche de Sodexo visant à démontrer, maintenir et surveiller la conformité aux normes européennes² applicables en matière de Protection des Données telles qu'énoncées dans le Règlement Général sur la Protection des Données (le « RGPD »)³ au sein du Groupe Sodexo et, plus particulièrement, par rapport aux flux transfrontaliers de Données Personnelles entre les entités Sodexo.

Cette Politique en tant que Sous-traitant s'applique à toutes les entités de Sodexo et à leurs employés (y compris les nouveaux employés) ainsi qu'à toute personne agissant en leur nom (consultants et prestataires individuels) et contient 26 Règles auxquelles Sodexo doit se conformer et respecter lors de la collecte et du Traitement des Données Personnelles en tant que Sous-traitant et également lors du transfert des données à des Responsables du Traitement ou à des sous-traitants au sein du Groupe Sodexo.

Les termes en majuscules utilisés dans la présente politique sont définis à l'Annexe 1.

La Politique en tant que Sous-traitant sera publiée sur le site internet accessible à l'adresse www.sodexo.com.

² Aux fins des présentes BCR, la référence à l'Europe signifie l'UE/EEE et la Suisse et « UE » ou « Européen » doit être interprété en conséquence.

³ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. (Règlement général de protection des données ou GRPD)

Qu'est-ce que le RGPD ?

Le RGPD donne aux personnes le droit de contrôler la manière dont leurs Données Personnelles sont utilisées.

Lorsque Sodexo collecte et traite les Données Personnelles des actuels ou anciens candidats à un emploi, employés, clients, consommateurs/bénéficiaires, fournisseurs, prestataires/sous-traitants, ou de tout autre tiers, cette activité est couverte et réglementée par le RGPD.

Dans le cadre du RGPD, les Données Personnelles désignent toute information relative à une personne physique identifiée ou identifiable (« Personne Concernée ») ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique (« Données Personnelles »).

Toute opération ou ensemble d'opérations effectuées par Sodexo sur les Données Personnelles collectées auprès des Personnes Concernées 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 tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (« Traitement » ou « Traitement des Données Personnelles »), relève de l'application du RGPD.

Le RGPD distingue les notions de « Responsable du Traitement » et de « Sous-traitant ». Le Responsable du Traitement détermine, seul ou conjointement avec d'autres, les finalités et les moyens du traitement des Données Personnelles (« Responsable du Traitement »). Le Sous-traitant, quant à lui, traite les Données Personnelles pour le compte du Responsable du Traitement (« Sous-traitant »).

Sodexo agit en tant que Responsable du Traitement dans les domaines où Sodexo détermine la finalité et les moyens du traitement des données, et Sodexo agit en tant que Sous-traitant lorsqu'il traite des Données Personnelles conformément aux instructions documentées du Responsable du Traitement de ces données.

Le RGPD impacte-t-il le flux transfrontalier des Données Personnelles au sein de Sodexo ?

Le RGPD s'applique non seulement aux entités Sodexo établies dans l'UE/EEE, mais également aux entités Sodexo établies en dehors de l'UE/EEE si : (a) elles offrent des biens ou des services à des Personnes Concernées de l'UE ; ou (b) le Traitement des Données Personnelles qui est effectué implique le suivi du comportement de Personnes Concernées de l'UE.

Le RGPD n'autorise pas le transfert transfrontalier des Données Personnelles dans des pays situés en dehors de l'Union Européenne qui n'assurent pas un niveau adéquat de Protection des Données. Certains des pays dans lesquels Sodexo opère ne sont pas considérés par la Commission européenne ou les autorités européennes de contrôle comme offrant un niveau de protection adéquat des libertés et des droits fondamentaux des personnes physiques dans le cadre des activités de traitement des données.

Quel est la finalité et le champ d'application des BCR de Sodexo ?

La finalité de ces BCR est de fournir une déclaration claire en matière de protection des Données Personnelles afin d'assurer un niveau de protection adéquat à toutes les Personnes Concernées conformément aux dispositions du RGPD.

La Politique en tant que Sous-traitant contient 26 Règles basées sur et interprétées conformément au RGPD, qui doivent être suivies par tous les employés de Sodexo (y compris les nouveaux employés et toutes les personnes agissant au nom et pour le compte de Sodexo, tels que les consultants et les prestataires individuels) des membres de la Politique en tant que Sous-traitant lorsqu'ils traitent les Données Personnelles, quel que soit le pays dans lequel ils se trouvent.

Cette Politique en tant que Sous-traitant aborde le Traitement des Données Personnelles des clients actuels, passés et des potentiels clients et des consommateurs/bénéficiaires de Sodexo, ainsi que du Traitement réalisé pour le compte d'un Client.

Le champ d'application territorial de la Politique en tant que Sous-traitant est la suivante : La Politique en tant que Sous-traitant encadre tous les flux de Données Personnelles traitées par Sodexo pour le compte d'un Client pour des activités de Traitement au sein du Groupe, quelle que soit l'origine des Données Personnelles.

Le champ d'application matériel de la Politique en tant que Sous-traitant est décrit à l'Annexe 7.

— Les pays de l'UE/EEE sont les suivants :

- Allemagne
- Autriche

- Belgique
- Bulgarie
- Chypre
- Danemark
- Espagne
- Finlande
- France
- Hongrie
- Irlande
- Italie
- Luxembourg
- Pays-Bas
- Norvège
- Pologne
- Portugal
- République tchèque
- Roumanie
- Suède

— Les pays tiers sont les suivants :

- Afrique du sud
- Algérie
- Australie
- Birmanie
- Brésil
- Canada
- Chili
- Chine continentale
- Colombie
- Costa-Rica
- Émirats Arabes Unis
- États-Unis
- Inde
- Indonésie
- Israël
- Japon
- Malaisie
- Mexique

- Maroc
- Nouvelle-Zélande
- Oman
- Panama
- Pérou
- Philippines
- République de Corée du Sud
- Royaume-Uni
- Singapour
- Sri Lanka
- Suisse
- Thaïlande
- Tunisie
- Turquie
- Uruguay
- Venezuela
- Vietnam

En pratique, qu'est-ce que cela signifie pour les Données Personnelles collectées et utilisées en Europe ?

Les Personnes Concernées dont les Données Personnelles sont traitées dans n'importe quel pays par une entité Sodexo agissant en tant que Sous-traitant et transférées au sein du Groupe Sodexo ont le droit de porter plainte, d'avoir recours à la justice et de demander une réparation appropriée et, le cas échéant, de recevoir une indemnisation, comme indiqué dans la Règle 21 pour toute violation de règles contenues dans la Politique en tant que Sous-traitant :

- (i) (i) qui sont directement opposables au Sous-traitant (obligation de respecter les instructions du Responsable du Traitement, obligation de mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriées, obligation de respecter les conditions lors de l'engagement d'un Sous-traitant ultérieur, obligation de coopérer avec le Responsable du Traitement et d'aider à se conformer et démontrer la conformité avec le RGPD, un accès facile aux BCR, la transparence lorsque la législation empêche le respect des BCR, le droit de porter plainte par le biais de mécanismes de plainte internes, la responsabilité et les devoirs de coopération avec les Autorités de Contrôle) ; et,
- (ii) (ii) qui sont opposables au Sous-traitant dans le cas où la Personne Concernée n'est pas en mesure d'intenter une action contre le Responsable du Traitement (obligation de respecter les BCR, droits des tiers bénéficiaires, responsabilité et charge de la preuve

avec Sodexo et non avec la Personne Concernée, accès facile aux BCR et transparence, traitement des réclamations, coopération avec les Autorités de Contrôle, liste des entités liées par les BCR, obligation de coopérer avec le Responsable du Traitement, transparence lorsque la législation empêche Sodexo de se conformer aux BCR et aux principes de Protection des Données).

Rôles dans le cadre de la Protection des Données

Le Délégué à la Protection des Données du Groupe Sodexo, ainsi que l'équipe dédiée à la Protection des Données du Groupe et le réseau de points de contact locaux dédiés à la Protection des Données (« Réseau global de Protection des Données») sont chargés de contrôler en interne le respect de la Politique en tant que Sous-traitant et de toutes autres politiques et procédures sous-jacentes.

Les opérationnels (désignés comme des experts de la Protection des Données dans les fonctions commerciales, les opérations de services et les segments) et les propriétaires d'applications informatiques sont chargés de veiller quotidiennement dans leur propre champ d'application que les entités de Sodexo respectent cette Politique.

Informations additionnelles

Sodexo SA, en tant que société multinationale basée en France, est l'une des entités centrales du Groupe Sodexo qui a demandé, pour elle-même et pour le compte des entités Sodexo du Groupe Sodexo, l'agrément de l'Autorité de Contrôle compétente, à savoir l'autorité française (Commission Nationale de l'Informatique et des Libertés ou CNIL ; www.cnil.fr).

Si vous avez des questions concernant les dispositions de la Politique en tant que Sous-traitant, vos droits en vertu de cette Politique ou tout autre sujet concernant la Protection des Données, vous pouvez contacter le Délégué à la Protection des Données du Groupe Sodexo qui traitera le problème ou le transmettra au point de contact local dédié à la Protection des Données pertinent ou aux opérationnels ou aux responsables informatiques au sein de Sodexo à l'adresse suivante :

Délégué à la Protection des Données du Groupe :

e-mail : dpo.group@sodexo.com

Adresse :

Délégué à la Protection des Données du Groupe
Équipe juridique du Groupe
Sodexo SA

255 quai de la Bataille de Stalingrad
92300, Issy-les-Moulineaux
France

Le Délégué à la Protection des Données du Groupe doit veiller à ce que les modifications apportées à la présente Politique en tant que Responsable du Traitement soient notifiées aux entités de Sodexo et aux personnes dont les Données Personnelles sont traitées par Sodexo via le site internet de Sodexo à l'adresse suivante : www.sodexo.com.

02

Les Règles



Les règles de la Politique en tant que Sous-traitant ont été divisées en deux Sections :

- La Section A traite des Règles de Protection des Données que Sodexo doit respecter lorsque Sodexo collecte et traite des Données Personnelles.
- La Section B traite des engagements concrets pris par Sodexo auprès des autorités européennes de contrôle pour garantir le caractère contraignant et efficace de la Politique en tant que Sous-traitant.

Section A

RÈGLE 1 - ÊTRE EN CONFORMITÉ AVEC LES BCR, LE RGPD ET LES RÉGLEMENTATIONS LOCALES APPLICABLES

RÈGLE 1.A - Sodexo se conforme avant tout aux dispositions de la Politique en tant que Sous-traitant, énoncées conformément au RGPD et à la législation locale applicable, qui exigent un niveau de protection plus élevé des Données Personnelles

Sodexo respecte les dispositions de la Politique en tant que Sous-traitant, énoncées conformément au RGPD et à la législation locale applicable si elle existe.

Lorsque la législation locale applicable exige un niveau de protection des Données Personnelles supérieur à celui du RGPD, cette législation locale applicable prévaut sur la Politique en tant que Sous-traitant.

Lorsqu'il n'y a pas de loi spécifique, ou lorsque cette loi n'atteint pas le niveau de protection des normes énoncées par les BCR, la position de Sodexo est de traiter les Données Personnelles conformément à la Politique en tant que Sous-traitant.

RÈGLE 1.B - Sodexo coopère et aide, dans la mesure du possible et dans un délai raisonnable, les Responsables du Traitement à se conformer à leurs obligations en vertu du RGPD et, le cas échéant, de la législation locale applicable qui exige un niveau de protection des Données Personnelles plus élevée.

Dans un délai raisonnable, et dans la mesure du possible, et comme l'exigent ses obligations contractuelles ou d'autres documents contraignants conclus avec un Responsable du Traitement (un Client), Sodexo coopère avec ce Responsable du Traitement (le Client), et l'aide à se conformer au RGPD et à la législation locale applicable.

RÈGLE 2 - GARANTIR LA LICÉITÉ, LA LOYAUTÉ ET LA TRANSPARENCE

RÈGLE 2.A - Sodexo aide le Responsable du Traitement à se conformer à ses obligations de licéité, de loyauté et de transparence.

Sodexo fournit une assistance au Responsable du Traitement (un Client) sur demande.

Sodexo assiste et coopère également avec le Responsable du Traitement pour répondre aux demandes et aux réclamations des Personnes Concernées (voir les Règles 25 et 17), pour informer les autres parties impliquées dans le Traitement des Données Personnelles, le cas échéant, afin que les Données Personnelles des Personnes Concernées soient exactes et tenues à jour (voir la Règle 5) et d'être en mesure de répondre à toute enquête ou requête des Autorités de Contrôle.

RÈGLE 2.B - Sodexo collecte et traite les Données Personnelles uniquement pour le compte et conformément aux instructions du Responsable du Traitement.

Sodexo ne collecte et ne traite les Données Personnelles que pour le compte et conformément aux instructions documentées (licites) reçues du Responsable du Traitement (un Client), comme spécifié dans le contrat de service, le contrat et tout autre document contraignant avec le Responsable du Traitement (un Client).

Si Sodexo n'est pas en mesure de se conformer à cette Règle, Sodexo en informe rapidement le Responsable du Traitement. Dans ce cas, le Responsable du Traitement est en droit de résilier la relation contractuelle avec Sodexo pour les services en lien avec le Traitement des Données Personnelles, sous réserve des conditions énoncées dans le contrat de service, le contrat ou tout autre document contraignant pertinent conclu avec le Responsable du Traitement (un Client). Si les conditions de Traitement des Données Personnelles sont susceptibles d'évoluer au cours de l'exécution des prestations fournies par Sodexo, Sodexo en informe le Responsable du Traitement qui aura la possibilité de s'opposer à cette modification ou de résilier le contrat, ou tout autre document contraignant pertinent avant la mise en œuvre d'un tel changement.

RÈGLE 3 - GARANTIR UNE LIMITATION DES FINALITÉS

RÈGLE 3 - Sodexo traite les Données Personnelles pour le compte du Responsable du Traitement pour une finalité connue, pertinente et fondée sur la loi déterminée par le Responsable du Traitement.

Les Données Personnelles sont traitées par Sodexo pour le compte du Responsable du Traitement, selon les finalités spécifiées, explicites et légitimes conformément aux instructions du Responsable du Traitement et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités, y compris en ce qui concerne les transferts de Données Personnelles vers un pays tiers, sauf si cela est requis par le RGPD ou la loi locale applicable à laquelle Sodexo est soumis en tant que Sous-traitant et qui exige un niveau de protection plus élevé pour les Données Personnelles. Dans un tel cas, Sodexo informe le Responsable du Traitement de cette exigence légale avant que le traitement n'ait lieu, à moins que la loi n'interdise une telle information pour un motif d'intérêt public important. Dans d'autres cas, si Sodexo en tant que Sous-traitant n'est pas en mesure d'assurer une conformité pour tout autre motif, il s'engage à en informer rapidement le Responsable du Traitement, auquel cas le Responsable du Traitement est en droit de suspendre les transferts de Données Personnelles impliquées et/ou de résilier le contrat ou tout autre document contraignant.

RÈGLE 4 - GARANTIR LA MINIMISATION DES DONNÉES

RÈGLE 4 - Sodexo ne traite que les Données Personnelles pertinentes et nécessaires à l'exécution des prestations.

Sodexo identifie la quantité minimale de Données Personnelles nécessaire pour satisfaire correctement la finalité des services tels que définis dans le contrat de service et tout autre document contraignant conclu avec le Responsable du Traitement (un Client).

RÈGLE - 5 GARANTIR L'EXACTITUDE

RÈGLE 5 - Sodexo assiste le Responsable du Traitement pour que les Données Personnelles soient exactes et, si nécessaire, mises à jour.

Sodexo et ses Sous-traitants (le cas échéant) agissent selon les instructions du Responsable du Traitement (un Client) afin que le Responsable du Traitement soit en conformité avec son obligation de maintenir les Données Personnelles exactes et, si nécessaire, à jour, corrigées ou supprimées.

Sodexo, agissant en tant que Sous-traitant, informe chaque entité Sodexo à laquelle les Données Personnelles ont été divulguées de toute rectification ou suppression de Données Personnelles.

Sur instruction du Responsable du Traitement et conformément aux dispositions de son contrat ou de tout autre document contraignant avec ce Responsable du Traitement, Sodexo et ses Sous-traitants ultérieurs (le cas échéant) doivent mettre en place les mesures nécessaires pour que les Données Personnelles soient supprimées ou anonymisées lorsque l'identification des données n'est plus nécessaire.

Sodexo, agissant en tant que Sous-traitant, informe chaque entité Sodexo à laquelle les Données Personnelles ont été divulguées de toute suppression ou anonymisation de Données Personnelles.

RÈGLE 6 - GARANTIR LA LIMITATION DE LA CONSERVATION

RÈGLE 6 - Sodexo aide le Responsable du Traitement à conserver les Données Personnelles aussi longtemps que nécessaire.

Les Données Personnelles sont toujours conservées et/ou effacées et/ou rendues anonymes selon les instructions du Responsable du Traitement (sous réserve que ces instructions soient conformes aux lois locales applicables) et conformément à la Politique Globale de collecte et de conservation des données de Sodexo (Annexe 2). Sodexo supprime les Données Personnelles de manière sécurisée conformément à la Politique de Sécurité des Systèmes d'Informations du Groupe⁴.

Lorsque la fourniture des services relatifs au Traitement des Données Personnelles prend fin, Sodexo en tant que Sous-traitant et ses sous-traitants ultérieurs (le cas échéant), suppriment,

⁴ Document interne

anonymisent ou restituent (selon le choix du Responsable du Traitement) toutes les Données Personnelles transférées et leurs copies au Responsable du Traitement, à moins que la législation locale applicable, la législation de l'UE/EEE, n'exige la conservation des Données Personnelles transférées. Dans ce cas, Sodexo informe le Responsable du Traitement et justifie qu'il garantira la confidentialité des Données Personnelles transférées et qu'il ne traitera plus activement les Données Personnelles transférées.

RÈGLE 7 - PRENDRE LES MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES APPROPRIÉES

RÈGLE 7.A - Sodexo adhère à la Politique de Sécurité des Systèmes d'Information du Groupe Sodexo et met en place les mesures techniques et organisationnelles telles que spécifiées dans le contrat de service, et tout autre document contraignant avec le Responsable du Traitement conformément à la législation locale applicable du Responsable du Traitement.

Sodexo respecte les exigences contenues dans la Politique de Sécurité des Systèmes d'Information du Groupe Sodexo⁵; qui est occasionnellement révisée et mise à jour, ainsi que toutes autres mesures de sécurité, d'intégrité et de confidentialité pertinentes à un domaine d'activité ou une fonction ainsi que toutes mesures de sécurité techniques et organisationnelles spécifiées dans le contrat ou tout autre document contraignant avec le Responsable du Traitement (un Client) qui protégeront les Données Personnelles contre la destruction ou la perte accidentelle ou illégale, l'altération, la divulgation ou l'accès non autorisé, en plus de la législation locale applicable du Responsable du Traitement.

Selon la nature du Traitement des Données Personnelles, ces mesures techniques et organisationnelles peuvent inclure le chiffrement des Données Personnelles, une révision périodique des mesures de sécurité, des installations de répétition et de sauvegarde des données et des tests de sécurité réguliers.

RÈGLE 7.B - Sodexo nomme un Sous-traitant ultérieur au sein du Groupe ou en externe avec l'autorisation écrite préalable, générale ou spécifique, du Responsable du Traitement et selon des engagements similaires à ceux énoncés dans le contrat avec le Responsable du Traitement et dans la Politique en tant que Sous-traitant.

Sodexo garantit que la Sous-traitance des Données Personnelles au sein du Groupe et/ou les transferts ultérieurs à des Sous-traitants externes sont effectués avec l'autorisation écrite, préalable et spécifique du Responsable du Traitement conformément à ses instructions (ex : autorisation générale ou spécifique, notification de changement, possibilité de s'opposer à toute

⁵ Document interne

modification ou de résilier le contrat) en ce qui concerne la désignation de Sous-traitants ultérieurs conformément aux dispositions du contrat de service, du contrat ou de tout autre document contraignant et est strictement lié à la finalité de l'exécution des services.

En cas de Sous-traitance au sein du Groupe, les Données Personnelles peuvent être sous-traitées par d'autres entités Sodexo liées par les BCR uniquement avec l'autorisation écrite, préalable, informée⁶ et spécifique du Responsable du Traitement.

Sodexo veille à ce que des informations à jour concernant sa nomination de Sous-traitants ultérieurs soient mises à la disposition du Responsable du Traitement conformément aux instructions contractuellement convenues avec le Responsable du Traitement.

Lorsque le Responsable du Traitement accepte la nomination de Sous-traitants ultérieurs, ces derniers seront désignés conformément à des engagements similaires à ceux énoncés dans le contrat entre Sodexo et le Responsable du Traitement, et dans tous les cas conformément à la Règle 7B et à la Politique en tant que Sous-traitant.

RÈGLE 7.C - Sodexo notifie toute violation des Données Personnelles au Responsable du Traitement sans retard injustifié conformément aux conditions convenues dans le cadre du contrat ou de tout autre document contraignant.

Sodexo notifie toute violation de Données Personnelles au Responsable du Traitement dans le délai convenu avec le Responsable du Traitement après en avoir pris connaissance et en tout état de cause sans retard injustifié.

Sodexo assiste le Responsable de Traitement pour identifier la nature de la violation des Données Personnelles, les conséquences probables de cette violation, propose ou prend des mesures pour remédier à la violation de Données Personnelles et assiste le Responsable du Traitement avec toute autre demande conformément aux instructions contractuellement convenues avec le Responsable du Traitement.

En outre, les Sous-traitants ultérieurs (le cas échéant) ont le devoir d'informer Sodexo agissant en tant que Sous-traitant ainsi que le Responsable du Traitement sans retard injustifié.

RÈGLE 7.D - Sodexo garantit que les Données Personnelles traitées pour le compte du Responsable du Traitement restent confidentielles.

Sodexo veille à ce que toutes les Données Personnelles qu'il traite restent confidentielles.

Sodexo garantit que toutes les personnes autorisées à traiter les Données Personnelles s'engagent à respecter une obligation de confidentialité appropriée.

⁶ Informations sur les principaux éléments (parties, pays, sécurité, garanties en cas de transferts internationaux, avec possibilité d'obtenir une copie du contrat utilisé).

RÈGLE 8 - PROTÉGER L'UTILISATION DES DONNÉES PERSONNELLES SENSIBLES ET DES AUTRES CATÉGORIES PARTICULIÈRES DE DONNÉES PERSONNELLES

RÈGLE 8 - Sodexo traite les Données Personnelles Sensibles et les autres catégories particulières de Données Personnelles uniquement en conformité avec les instructions licites écrites et documentées du Responsable du Traitement et ne traite pas ces données à d'autres fins.

Sodexo traite les Données Personnelles Sensibles et les autres catégories particulières de Données Personnelles uniquement en conformité avec les instructions licites écrites et documentées du Responsable du Traitement et ne traite pas ces données à d'autres fins.

Si Sodexo n'est pas en mesure de traiter ces Données Personnelles conformément avec les instructions du Responsable du Traitement, il en informe rapidement le Responsable du Traitement. Le Responsable du Traitement sera en droit de résilier la relation contractuelle avec Sodexo et Sodexo se conformera aux instructions du Responsable du Traitement concernant la restitution, l'anonymisation et la destruction des Données Personnelles conformément à la Règle 6.

RÈGLE 9 - CONSERVER LES REGISTRES DES ACTIVITÉS DE TRAITEMENT DES DONNÉES

RÈGLE 9 - Sodexo conserve des registres de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable du Traitement.

Sodexo conserve des registres de ses activités de traitement effectuées pour le compte du Responsable du Traitement, qui comprennent entre autres une description générale des mesures de sécurité mises en œuvre concernant les Données Personnelles traitées pour le compte du Responsable du Traitement.

Ces registres comprennent les éléments suivants conformément à l'Article 30, paragraphe 2, du RGPD :

- (i) le nom et les coordonnées de l'entité Sodexo agissant en tant que Sous-traitant, chaque Responsable du Traitement pour le compte duquel l'entité Sodexo agit et du Délégué à la Protection des Données ;
- (ii) les catégories de traitement effectuées pour le compte de chaque Responsable du Traitement ;
- (iii) le cas échéant, les transferts transfrontaliers de Données Personnelles vers un pays tiers, y compris l'identification de ce pays tiers et, dans le cas de transferts vers des pays tiers qui ne sont pas reconnus comme pays adéquats, la documentation des garanties appropriées ;
- (iv) si possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'Article 32, paragraphe 1, pour assurer un niveau de sécurité adapté au risque, y compris notamment, le cas échéant :
 - a. la pseudonymisation et le chiffrement des Données Personnelles ;
 - b. la capacité d'assurer en continu la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement ;
 - c. la possibilité de rétablir la disponibilité et l'accès aux Données Personnelles en temps opportun en cas d'incident physique ou technique ;
 - d. un processus pour tester et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement

Sur demande, ces registres seront communiqués aux Autorités de contrôle compétentes ou au Responsable du Traitement.

Sodexo, en tant que Sous-traitant, met à la disposition du Responsable du Traitement toutes les informations nécessaires pour démontrer le respect de leurs obligations respectives, permet et contribue à la réalisation d'audits, y compris les inspections menées par le Responsable du Traitement ou par un tiers mandaté par le Responsable du Traitement. En outre, Sodexo informe immédiatement le Responsable du Traitement s'il pense que des instructions enfreignent le RGPD ou toute autre réglementation locale applicable.

RÈGLE 10 - RESPECTER LES DROITS DES PERSONNES CONCERNÉES

RÈGLE 10 - Sodexo assiste le Responsable du Traitement pour répondre aux droits des Personnes Concernées.

Sodexo et ses Sous-traitants (le cas échéant) exécutent, dans la mesure du possible, toutes les mesures techniques et organisationnelles appropriées, à la demande du Responsable du Traitement, pour que ce dernier puisse se conformer à ses obligations et permettre aux Personnes Concernées d'exercer leurs droits, notamment, dans la mesure autorisée par la législation de l'EEE/UE, en informant rapidement le Responsable du Traitement si une Personne Concernée demande l'accès, la rectification, l'effacement, la limitation, la portabilité, l'opposition au Traitement de ses Données Personnelles.

Sodexo ne répond directement à aucune demande de la Personne Concernée sans l'accord écrit préalable du Responsable du Traitement.

Sodexo fournit au Responsable du Traitement une coopération, une assistance et des informations utiles concernant la demande d'une Personne Concernée afin d'aider le Responsable du Traitement à se conformer à son obligation de respecter les droits des Personnes Concernées, dans la mesure autorisée par la loi et dans la mesure où le Responsable du Traitement n'a pas accès à ces Données Personnelles par le biais de leur utilisation pour les services fournis par Sodexo ou ses sous-traitants (le cas échéant).

Si Sodexo a été chargé par le Responsable du Traitement de fournir une adresse e-mail générique pour permettre aux Personnes Concernées d'exercer leurs droits, Sodexo pourrait en outre être directement contacté par les Personnes Concernées, à condition que le Responsable du Traitement ait fourni les informations pertinentes aux Personnes Concernées conformément au RGPD.

La Personne Concernée a le droit de déposer une plainte auprès de l'autorité de contrôle et également auprès des tribunaux conformément à la Règle 17 de la Politique en tant que Sous-traitant.

RÈGLE 11 - RESPECTER LES CONDITIONS RELATIVES AU PROFILAGE ET AUX PRISES DE DÉCISIONS INDIVIDUELLES ENTIÈREMENT AUTOMATISÉES ET METTRE EN ŒUVRE LES SAUVEGARDES APPROPRIÉES

La Règle 11 ne s'applique pas aux Sous-traitants.

RÈGLE 12 - TRANSPARENCE ET INFORMATIONS DE LA PERSONNE CONCERNÉE

RÈGLE 12 - Sodexo met la Politique en tant que Sous-traitant à la disposition du Responsable du Traitement.

La Politique en tant que Sous-traitant est mise à la disposition des Personnes Concernées sur le site officiel de Sodexo. Par ailleurs, la Politique Globale de Sodexo relative à la Protection des Données Personnelles (Annexe 5) comprend une clause dédiée aux droits des tiers bénéficiaires.

La Politique en tant que Sous-traitant est également disponible et opposable au Responsable du Traitement car elle sera incluse par référence dans les accords de traitement de données conclus avec les Clients ou tout autre document contraignant. L'accord de traitement de données ou tout autre document contraignant conclu avec les Clients contient (i) l'engagement du Responsable du Traitement concernant le fait que si le transfert concerne des catégories particulières de données, la Personne Concernée a été ou sera informée avant le transfert que ses données peuvent être transmises à un pays tiers n'assurant pas une protection adéquate ; (ii) l'engagement du Responsable du Traitement d'informer la Personne Concernée de l'existence de Sous-traitants basés en dehors de l'UE et l'existence des BCR ; (iii) l'engagement du Responsable du Traitement à mettre à la disposition des Personnes Concernées sur demande une copie des BCR et une copie de l'accord de traitement des données ou de tout autre document contraignant.

RÈGLE 13 - ASSURER UNE PROTECTION ADÉQUATE POUR LE TRANSFERT TRANSFRONTALIERS DE DONNÉES PERSONNELLES

RÈGLE 13 - Sodexo ne transfère pas de Données Personnelles à des tiers situés en dehors de l'UE/EEE sans assurer une protection adéquate des Données Personnelles transférées.

Lorsque les Données Personnelles sont transférées à un tiers, l'entité Sodexo transférant les Données Personnelles en tant que Sous-traitant :

- obtient le consentement préalable du Responsable du Traitement pour un tel transfert à un tiers ;
- garantit dans un contrat de service ou tout autre document contraignant tel qu'un accord de traitement de données avec le tiers que ledit tiers s'engage par écrit à fournir des garanties suffisantes conformément au RGPD et aux directives du CEPD ;

- signe le module 3 des clauses contractuelles types de la Commission européenne⁷ (transfert de sous-traitant à sous-traitant) et, si nécessaire, met en œuvre les mesures supplémentaires nécessaires conformément à Schrems II.

RÈGLE 14 - RESPECT DE LA PROTECTION DES DONNEES DÈS LA CONCEPTION ET PAR DÉFAUT

RÈGLE 14 - Sodexo assiste le Responsable du Traitement dans la mise en œuvre des mesures techniques et organisationnelles appropriées pour se conformer aux principes de Protection des Données et faciliter la Protection des Données dès la conception et par défaut.

Sodexo assiste le Responsable du Traitement dans la mise en œuvre des mesures techniques et organisationnelles appropriées pour se conformer aux principes de Protection des Données et faciliter la Protection des Données dès la conception et par défaut.

RÈGLE 15 - EFFECTUER UNE ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNÉES (AIPD)

RÈGLE 15 - Sodexo aide le Responsable du Traitement à effectuer les analyses d'impact requises relatives à la Protection des Données.

Conformément aux articles 35 et 36 et au considérant 95 du RGPD, Sodexo fournit une assistance raisonnable telle que définie dans la contrat de service ou tout autre document contraignant avec le Responsable du Traitement, pour mettre à disposition les informations relatives au Traitement des Données Personnelles qu'il traite en son nom, pour s'assurer que le Responsable du Traitement respecte les obligations de réaliser une AIPD et d'une consultation préalable de l'autorité de contrôle, si nécessaire et sur demande.

⁷ Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil

Section B

RÈGLE 16 - FORMATION ET SENSIBILISATION

RÈGLE 16 - Sodexo dispense une formation aux employés qui ont un accès permanent ou régulier aux Données Personnelles et/ou qui sont impliqués dans la collecte de Données Personnelles ou dans le développement d'outils utilisés pour traiter les Données Personnelles pour le compte du Responsable du Traitement.

Un programme de formation complet

Pour rendre la Politique en tant que Sous-traitant opposable et efficace l'équipe dédiée à la Protection des Données du Groupe a mis en place un programme de formation complet qui explique les principes régissant le Traitement des Données Personnelles dans le cadre de cette Politique.

Un module général est destiné à fournir une formation de base sur les principes relatifs à la Protection des Données à tous les employés de Sodexo, tandis que des modules spécifiques sont destinés aux employés des entités Sodexo qui ont un accès permanent ou régulier aux Données Personnelles et/ou sont impliqués dans la collecte de Données Personnelles ou dans la sélection ou le développement des outils utilisés pour traiter les Données Personnelles. En outre, les employés d'une entité de Sodexo doivent être informés de leurs obligations de se conformer aux politiques de Protection des Données de Sodexo dans le cadre du Code de Conduite - Principes d'intégrité de Sodexo⁸.

Les modules sont mis à jour régulièrement pour mieux refléter les activités de Sodexo et faire comprendre aux collaborateurs comment gérer quotidiennement la Protection des Données Personnelles dans le cadre de leurs fonctions

De plus, les points de contact locaux dédiés à la Protection des Données dispensent une formation conforme à la législation locale en tenant compte de leurs exigences spécifiques.

Suivi du programme de formation

Les entités Sodexo prennent des mesures raisonnables et appropriées pour communiquer avec leurs employés et pour fournir une formation appropriée sur les exigences de la Politique en tant que Sous-traitant.

⁸ Document Interne

L'achèvement du programme de formation sur la Protection des Données est contrôlé par l'équipe dédiée à la Protection des Données du Groupe et le point de contact local dédié à la Protection des Données, ainsi que par les équipes globales et locales Talents et Développement.

RÈGLE 17 - GERER LES DROITS RELATIFS A LA PROTECTION DES DONNÉES

RÈGLE 17 - Sodexo assiste le Responsable du Traitement pour répondre à une demande ou à une plainte qu'il a reçue.

Lorsqu'un point de contact local dédié à la Protection des Données reçoit une demande émanant d'une Personne Concernée ou une réclamation émanant de l'Autorité de Contrôle relative à un Traitement de Données Personnelles effectué pour le compte d'un Responsable de Traitement, il doit la communiquer au Responsable de Traitement concerné sans retard injustifié (ou dans le délai de notification convenu avec le Responsable du Traitement) et sans obligation de la traiter (sauf indication contraire du Responsable du Traitement).

Le rôle du point de contact local dédié à la Protection des Données est de traiter les demandes des Personnes Concernées et les plaintes des Autorités de Contrôle uniquement sur instruction du Responsable du Traitement ou si le Responsable du Traitement a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable.

Si le Responsable du Traitement a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, Sodexo traite la demande sans retard excessif et en tout état de cause dans un délai d'un mois après réception de la demande, ou si nécessaire, en raison de la complexité et du nombre de demandes dans un délai prolongé de 3 mois (1 + 2) maximum, après avoir informé la Personne Concernée d'une telle prorogation dans un délai d'un mois à compter de la réception de la demande, accompagnée des motifs du retard, conformément à l'Article 12.3 du RGPD. Si la demande a été faite par voie électronique, les informations sont fournies dans la mesure du possible par voie électronique sauf demande contraire de la personne concernée.

Dans ce cas, les Personnes Concernées sont informées des étapes pratiques du système de gestion des demandes et des réclamations dans les politiques locales de Protection des Données mettant en œuvre la Politique Globale de gestion des droits des Personnes Concernées décrite à l'Annexe 6.

RÈGLE 18 - ÉVALUER LA CONFORMITÉ : PROGRAMME D'AUDIT

RÈGLE 18 - Sodexo répond aux demandes d'audit du Responsable de Traitement.

Selon le programme global d'audit des BCR de Sodexo, Sodexo audite la conformité du Groupe Sodexo avec la Politique en tant que Sous-traitant, et en particulier met en œuvre un plan d'audit qui couvre tous les aspects de la Politique en tant que Sous-traitant, y compris les méthodes pour s'assurer que des actions correctives auront lieu.

Les audits Sodexo sont réalisés annuellement par l'équipe de Contrôle Interne et l'équipe d'Audit Interne du Groupe, ou si besoin sur demande spécifique du Délégué à la Protection des Données du Groupe.

Les auditeurs internes peuvent être assistés par des auditeurs externes, en cas de besoin.

Les résultats de tous les audits doivent être communiqués au Délégué à la Protection des Données du Groupe, au point de contact local dédié à la Protection des Données et au conseil d'administration du Groupe Sodexo ; et aux membres concernés du comité de direction du Groupe.

Les actions correctives sont décidées en fonction de ce rapport.

Sodexo permet aux Autorités de Contrôle compétentes d'accéder aux résultats des audits internes sur demande et de réaliser un audit de Protection des Données de toute entité de Sodexo si nécessaire.

Sodexo répond aux demandes d'audit des responsables du traitement comme convenu dans les accords de service, les contrats ou tout autre document contraignant conclus avec les Responsables du Traitement.

Les entités de Sodexo agissant en tant que Sous-traitants ou leurs sous-traitants ultérieurs acceptent, à la demande écrite du Responsable du Traitement, de soumettre leurs installations de traitement de données à un audit des activités de traitement qui peut être effectué soit par le Responsable du Traitement soit par un organisme de contrôle composé de membres indépendants et possédant les qualifications professionnelles requises, tenus par un devoir de confidentialité, choisis par le Responsable du Traitement, le cas échéant, en accord avec l'Autorité de Contrôle.

RÈGLE 19 - SUIVRE L'APPLICATION DES BCR

RÈGLE 19 - Sodexo surveille la mise en œuvre des BCR.

Pour assurer la mise en œuvre efficace de la Politique en tant que Sous-traitant, l'équipe dédiée à la Protection des Données du Groupe a établi un registre des risques.

En outre, chaque point de contact local dédié à la Protection des Données reporte les meilleures pratiques locales pour mettre en œuvre la Politique en tant que Sous-Traitant et les analyses d'impact relatives à la Protection des Données effectuées localement à l'équipe dédiée à la Protection des Données du Groupe de manière trimestrielle. Les rapports des points de contact locaux dédiés à la Protection des Données sont centralisés et analysés l'équipe dédiée à la Protection des Données du Groupe. Les résultats de l'analyse font partie du rapport annuel remis au Comité de Direction de Sodexo.

RÈGLE 20 - ÉQUIPE DÉDIÉE À LA PROTECTION DES DONNÉES DU GROUPE ET RÉSEAU DE POINTS DE CONTACT LOCAUX

RÈGLE 20 - Sodexo garantit le respect de la Politique en tant que Sous-traitant par le biais d'une structure de Gouvernance de la Protection des Données.

Pour superviser et garantir le respect de la Politique en tant que Sous-traitant, Sodexo a mis en place, avec le soutien de son Comité de Direction, une structure de Gouvernance de la Protection des Données comme suit :

- un Délégué à la Protection des Données du Groupe désigné conformément à l'Article 37 du RGPD rattaché au Directeur Juridique du Groupe ;
- l'équipe dédiée à la Protection des Données du Groupe est composée de juristes en Protection des Données au niveau global, accompagnant l'équipe du Délégué à la Protection des Données du Groupe dans ses missions ;
- un réseau de point de contact dédié à la Protection des Données au niveau local (« DP SPOC local »).

Le rôle du Délégué à la Protection des Données du Groupe est de surveiller la conformité au niveau mondial et d'évaluer l'efficacité du programme de Protection des Données de Sodexo (collecter des informations pour identifier les activités de traitement, analyser et vérifier la

conformité, etc.). Le Délégué à la Protection des Données du Groupe fournit à la direction générale des conseils et des recommandations ainsi qu'un rapport annuel sur les activités de l'équipe dédiée à la Protection des Données du Groupe. En outre, le rôle de l'équipe dédiée à la Protection des Données du Groupe est de surveiller la conformité au niveau mondial et d'évaluer l'efficacité du programme Global de Conformité à la Protection des Données de Sodexo.

Le Délégué à la Protection des Données du Groupe conseille et assiste au besoin les DP SPOCs locaux pour se conformer au Programme global de Protection des Données de Sodexo, pour traiter les enquêtes des Autorités de Contrôle et s'assure que le DP SPOC local gère les plaintes locales des Personnes Concernées conformément à la Règle 17, signale au Délégué à la Protection des Données du Groupe les problèmes majeurs liés à la Protection des Données, vérifie la conformité au niveau local et est disponible, dans la langue locale, aux Personnes Concernées, au Responsable du Traitement (un Client) et à l'Autorité de Contrôle locale.

RÈGLE 21 - DROITS DES TIERS BÉNÉFICIAIRES

RÈGLE 21 - Sodexo confère expressément des droits aux Personnes Concernées soit lorsque ces droits sont directement opposables à Sodexo, soit lorsque les droits sont opposables à Sodexo dans le cas où la Personne Concernée n'est pas en mesure d'intenter une action contre le Responsable du Traitement.

1. Droits directement opposables à Sodexo en tant que Sous-traitant :

Les Personnes Concernées sont en mesure d'appliquer la Politique en tant que Sous-traitant à l'encontre des entités Sodexo agissant en tant que Sous-traitants et notamment :

- L'obligation de respecter les instructions du Responsable du Traitement concernant le traitement des Données Personnelles, y compris pour les transferts de Données Personnelles vers des pays tiers ;**
- L'obligation de mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées et l'obligation de notifier toute Violation des Données Personnelles au Responsable du Traitement (Règle 7) ;**
- L'obligation de respecter les conditions lors de l'engagement d'un sous-traitant ultérieur à l'intérieur ou à l'extérieur du Groupe (Règle 7) ;**
- L'obligation de coopérer avec le Responsable du Traitement et de l'aider à se conformer et à démontrer le respect de la législation, par exemple pour répondre aux demandes des Personnes Concernées concernant leurs droits (Règles 1B, 2A, 5, 10, 17 et 23) ;**

- **Transparence de la Politique en tant que Sous-traitant** : Les Personnes Concernées ont un accès facile à leurs droits de tiers bénéficiaires puisque la Politique en tant que Sous-traitant est disponible sur l'intranet et le site internet officiel de Sodexo. Ils peuvent obtenir une copie de cette politique sur demande auprès des membres des BCR agissant en tant que Sous-traitants. Par ailleurs, la Politique Globale de Sodexo relative à la Protection des Données Personnelles (Annexe 5) comprend une annexe dédiée sur les droits des tiers bénéficiaires.

- **Transparence sur les cas où la législation nationale empêche le Groupe Sodexo de se conformer aux BCR** : ils peuvent appliquer la Règle 23.

- **Droit d'introduire une Réclamation** : Lorsqu'un point de contact local dédié à la Protection des Données reçoit une Réclamation d'une Personne Concernée relativement à un Traitement de Données Personnelles effectué pour le compte d'un Responsable du Traitement, il la communique sans délai au Responsable du Traitement concerné sans obligation de la traiter. Le point de contact local dédié à la Protection des Données traite les Réclamations de cette Personne Concernée uniquement sur instruction du Responsable du Traitement ou si le Responsable du Traitement a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable. Dans ce cas, les Personnes Concernées sont informées des étapes pratiques du système de gestion des demandes et des réclamations dans les politiques locales de Protection des Données mettant en œuvre la Politique Globale de gestion des droits des Personnes Concernées décrite à l'Annexe 6. Les Personnes Concernées reçoivent les informations suivantes : (i) où se plaindre ; (ii) sous quelle forme ; (iii) le délai de réponse à la plainte ; (iv) les conséquences si la réclamation est rejetée ; (v) les conséquences si la réclamation est considérée comme justifiée ; (vi) le droit de déposer une réclamation devant le Tribunal ou l'Autorité de Contrôle compétente.

- **Coopération** : les Personnes Concernées peuvent opposer la Règle 24.

- **Responsabilité** : Sodexo SA, en tant que siège européen de Sodexo agissant en tant que Sous-traitant, accepte la responsabilité et s'engage à prendre les mesures nécessaires pour remédier aux actes d'autres entités Sodexo établies en dehors de l'UE/EEE ou aux violations causées par un Sous-traitant externe établi en dehors de l'UE/EEE, à verser une indemnisation pour tout dommage résultant d'une violation des BCR ou à démontrer que ces entités Sodexo établies en dehors de l'UE/EEE ne sont pas responsables de la violation ou que les violations causées par le Sous-traitant externe n'ont pas eu lieu. La société Sodexo SA susmentionnée qui a accepté la responsabilité aura la charge de démontrer que l'entité Sodexo en dehors de l'UE/EEE n'est pas responsable de la violation des règles ayant conduit la Personne Concernée à réclamer des dommages et intérêts. Si elle est en mesure de prouver que ladite entité Sodexo n'est pas responsable du fait générateur du dommage, elle pourra se dégager de toute responsabilité.

2. Droits opposables à Sodexo en tant que Sous-traitant si la Personne Concernée n'est pas en mesure d'intenter une action contre le Responsable du Traitement :

Les Personnes Concernées couvertes par le champ d'application de la Politique en tant que Sous-traitant sont des tiers bénéficiaires en vertu de cette Règle, qui est rendue opposables par l'accord intra-groupe d'adhésion signé entre les entités du Groupe Sodexo.

Pour être opposée par le Responsable du Traitement, la Politique en tant que Sous-traitant sera incluse dans le contrat de service, le contrat ou tout autre document contraignant signé entre une entité Sodexo agissant au nom d'un Responsable du Traitement et ledit Responsable du Traitement (un Client).

Les Personnes Concernées ont le droit de faire respecter la Politique en tant que Sous-traitant contre le Responsable du Traitement pour le compte duquel les Données Personnelles sont traitées par Sodexo en déposant une plainte auprès de l'Autorité de Contrôle compétente ou devant un tribunal compétent pour le Responsable du Traitement de l'UE/EEE.

Toutefois, les Personnes Concernées peuvent appliquer les Règles énoncées dans la Politique en tant que Sous-traitant en tant que tiers bénéficiaires lorsqu'elles ne sont pas en mesure d'intenter une action contre le Responsable du Traitement en cas de violation de l'un des engagements de la Politique en tant que Sous-traitant par une entité Sodexo (ou par un Sous-traitant ultérieur) agissant en tant que Sous-traitant (par exemple, si le Responsable du Traitement a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, à moins qu'une entité successeur n'ait assumé l'intégralité des obligations légales du Responsable du Traitement par contrat ou de plein droit, auquel cas les Personnes Concernées peuvent faire valoir leurs droits à l'encontre de cette entité).

Dans ce cas, les Personnes Concernées peuvent au moins appliquer les règles suivantes contenues dans la Politique en tant que Sous-traitant :

- L'obligation de respecter les BCR (Règle 1) ;
- Les Droits des tiers bénéficiaires (Règle 21) ;
- Responsabilité et charge de la preuve incombant à Sodexo et non à la personne concernée (Règle 22) ;
- L'accès facile au BCR et leur transparence (Règle 12) ;
- Le traitement des plaintes (Règle 17) ;
- La coopération avec l'Autorité de Contrôle (Règle 24) ;
- Le transfert des Données Personnelles (Règle 13) ;
- La liste des entités liées par les BCR ;
- L'obligation de coopérer avec le Responsable du Traitement (Règle 1) ;
- La transparence, la loyauté et la licéité (Règle 2) ;
- La limitation de la finalité (Règle 3) ;
- La qualité des données (Règles 4, 5 et 6) ;
- La sécurité (Règle 7) ;
- Les droits de la Personne Concernée (Règle 10) ;
- Les conditions liées à la sous-traitance (Règle 7B) ;

- La transparence lorsque la législation nationale empêche le Groupe de se conformer aux BCR (Règle 23).

3. Dispositions en matière d'indemnisation et de juridiction (pour les droits des Personnes Concernées 1. et 2.)

Les Personnes Concernées peuvent introduire une réclamation (i) auprès de l'Autorité de Contrôle française (la « Commission Nationale de l'Informatique et des Libertés », la « CNIL ») contre Sodexo SA, responsable de l'exportation des données (a) auprès de l'Autorité de Contrôle dans l'Etat Membre de leur résidence habituelle, (b) de leur lieu de travail ou (c) du lieu de l'infraction alléguée et ii) devant les tribunaux compétents français où Sodexo SA a son siège social ou devant les tribunaux compétents des États Membres de l'UE/EEE où ils ont leur résidence. Lorsque Sodexo en tant que Sous-traitant et le Responsable du Traitement impliqués dans le même traitement de Données Personnelles sont reconnus responsables de tout dommage causé par un tel traitement, les Personnes Concernées ont le droit de recevoir une indemnisation pour l'intégralité du dommage directement de la part de Sodexo agissant en qualité de Sous-traitant.

RÈGLE 22 - RESPONSABILITÉ

RÈGLE 22 - Sodexo respecte les règles suivantes en matière de responsabilité.

Lorsqu'une Personne Concernée subit un dommage car le traitement des Données Personnelles de Sodexo n'est pas-conforme avec la Politique en tant que Sous-traitant, le Responsable du Traitement conserve la responsabilité de se conformer au RGPD. Les Responsables du Traitement qui entrent dans le champ d'application du RGPD transmettront certaines obligations de Protection des Données à Sodexo dans les accords de service, contrats ou autres documents contraignants que Sodexo a conclu avec eux. Par conséquent, si Sodexo ne se conforme pas aux instructions du Responsable du Traitement concernant le traitement des Données Personnelles telles qu'énoncées dans le contrat de service ou tout autre document contraignant conclu avec un Responsable du Traitement, le Responsable du Traitement pourrait être en violation du RGPD et du contrat de service, et Sodexo peut faire face à une réclamation pour rupture de contrat, qui pourrait entraîner le paiement d'une indemnisation pour tout dommage matériel ou immatériel/dommage moral ou d'autres recours judiciaires.

Dans de tels cas, si un Responsable du Traitement démontre qu'il a subi un dommage et qu'il est probable que le dommage soit survenu en raison d'une violation de la Politique en tant que Sous-traitant par une entité Sodexo en dehors de l'Europe (ou un Sous-traitant tiers établi en dehors de l'Europe), ce Responsable du Traitement a le droit d'opposer la Politique en tant que Sous-traitant à Sodexo SA, en tant que siège européen de Sodexo.

Sodexo SA acceptera la responsabilité et s'engage à prendre les mesures nécessaires pour remédier aux actes d'autres entités Sodexo établies en dehors de l'UE/EEE ou aux violations causées par un Sous-traitant externe établi en dehors de l'UE/EEE, à verser une indemnisation pour tout dommage résultant d'une violation des BCR, ou à démontrer que ces entités Sodexo établies en dehors de l'UE/EEE ne sont pas responsables de la violation ou que les violations causées par le Sous-traitant externe n'ont pas eu lieu. En outre, Sodexo SA devra démontrer que l'entité Sodexo en dehors de l'UE/EEE n'est pas responsable de la violation des règles ayant conduit la Personne Concernée à réclamer des dommages et intérêts. Si elle est en mesure de prouver que ladite entité Sodexo n'est pas responsable du fait générateur du dommage, elle pourra se dégager de toute responsabilité.

03

Dispositions finales



RÈGLE 23 - ACTIONS EN CAS DE REGLEMENTATIONS OU PRATIQUES NATIONALES EMPÊCHANT LE RESPECT DES BCR – DEMANDE JURIDIQUEMENT CONTRAIGNANTE DE COMMUNICATION DES DONNÉES PERSONNELLES

RÈGLE 23.A - Sodexo procède à une évaluation de la législation et des pratiques locales applicables avant tout transfert de Données Personnelles afin de s'assurer qu'elles ne l'empêchent pas de remplir ses obligations en vertu de la Politique en tant que Sous-traitant et qu'elles n'ont pas un effet substantiel sur sa capacité à se conformer à cette politique.

RÈGLE 23.B - Sodexo s'assure que lorsqu'il a des raisons de croire que la législation ou les pratiques locales applicables l'empêchent de remplir ses obligations en vertu de la Politique en tant que Sous-traitant et qu'elles ont un effet substantiel sur sa capacité à se conformer à la présente Politique en tant que Sous-traitant, il en informe rapidement le Responsable du Traitement et/ou Sodexo SA ou le membre des BCR situé dans l'UE/EEE ou le Délégué à la Protection des Données du Groupe et tout autre point de contact local dédié à la Protection des Données pertinent et l'entité Sodexo agissant en tant qu'Exportateur de Données.

RÈGLE 23.C - Sodexo s'assure que lorsqu'il reçoit une demande juridiquement contraignante de communication des Données Personnelles soumises à la Politique en tant que Sous-traitant, il en informe rapidement Sodexo SA, le Délégué à la Protection des Données du Groupe, l'entité Sodexo agissant en tant qu'Exportateur de Données, le Responsable du Traitement (par l'intermédiaire de l'entité Sodexo agissant en tant qu'Exportateur de Données), et si possible, la Personne Concernée s'il en reçoit l'instruction du Responsable du Traitement, sauf si une autorité chargée de l'application de la loi l'interdit ; et met la demande en attente sauf si une autorité ou un organisme chargé de l'application de la loi l'interdit. La notification comprendra, entre autres, des informations sur les données demandées, le nombre de demandes, l'organisme demandeur et la base juridique de la divulgation.

Évaluation de la législation et des pratiques locales applicables

Conformément aux recommandations du CEPD⁹ ; et aux Clauses Contractuelles types de l'Union européenne¹⁰:

Les entités de Sodexo garantissent qu'elles n'ont aucune raison de croire que la législation et les pratiques locales applicables les empêchent de remplir leurs obligations en vertu de la Politique

⁹ Recommandations 01/2020 sur les mesures qui complètent les outils de transfert pour assurer le respect du niveau européen de protection des données personnelles adoptées le 18 juin 2021.

¹⁰ Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu règlement (UE) 2016/679 du Parlement européen et du Conseil

en tant que Sous-traitant ou leurs obligations contractuelles avec le Responsable du Traitement et qu'elles n'ont pas un effet substantiel sur leur capacité à se conformer à cette politique ou à leurs obligations. Ceci est basé sur leur compréhension que les lois et pratiques locales applicables qui respectent l'essence des libertés et droits fondamentaux et n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour sauvegarder l'une des finalités énumérées à l'Article 23, paragraphe 1, du RGPD, ne sont pas en contradiction avec la Politique en tant que Sous-traitant.

Sodexo déclare qu'en fournissant cette garantie, il a dûment tenu compte, avec le concours du Délégué à la Protection des Données du Groupe, notamment des éléments suivants :

- les circonstances spécifiques du transfert, y compris la longueur de la chaîne de traitement, le nombre d'acteurs impliqués et les canaux de transmission utilisés ; les transferts ultérieurs prévus ; le type de destinataire ; la finalité du traitement ; les catégories et le format des Données Personnelles transférées ; le secteur économique dans lequel le transfert a lieu ; le lieu de stockage des données transférées ;
- les lois et pratiques de la législation locale applicable - y compris celles exigeant la communication de données aux autorités publiques ou autorisant l'accès à de telles autorités - pertinentes à la lumière des circonstances spécifiques du transfert, des limitations et garanties applicables, et du caractère exécutoire du droit de la personne concernée et l'efficacité des recours juridiques par les personnes concernées ;
- toutes les garanties contractuelles, techniques ou organisationnelles pertinentes mises en place pour compléter les garanties prévues par la Politique en tant que Sous-traitant et conformément aux instructions du Responsable du Traitement, y compris les mesures appliquées lors de la transmission et du traitement des Données Personnelles au sein des entités de Sodexo.

Les entités de Sodexo acceptent de documenter cette évaluation et de la mettre à la disposition du Responsable du Traitement et de l'autorité de contrôle compétente sur demande.

Lorsqu'une entité de Sodexo a des raisons de croire que la législation et/ou les pratiques locales applicables ou une demande de communication peuvent l'empêcher de remplir ses obligations en vertu de la Politique en tant que Sous-traitant ou ses obligations contractuelles avec le Responsable du Traitement et ont un effet substantiel sur sa capacité à se conformer à la présente Politique en tant que Sous-traitant ou à ses obligations contractuelles avec le Responsable du Traitement, il informe sans délai, conformément au contrat de service ou à tout autre document contraignant conclu avec le Responsable du Traitement (un Client) :

- L'entité Sodexo agissant en tant qu'Exportateur de Données, qui transmettra la notification au Responsable du Traitement, qui a le droit de suspendre le transfert de Données Personnelles et/ou de résilier le contrat ou tout autre document contraignant avec Sodexo ; et,
- Sodexo SA ou,

- Le Délégué à la Protection des Données du Groupe et tout autre point de contact local dédié à la Protection des Données pertinent.

Suite à cette notification, Sodexo SA et l'entité Sodexo agissant en tant qu'Exportateur de Données doivent rapidement, avec l'aide du Délégué à la Protection des Données du Groupe et, si nécessaire, le point de contact local dédié à la Protection des Données pertinent et, le cas échéant, en consultation avec le Responsable du Traitement, identifier les mesures appropriées (ex : mesures techniques ou organisationnelles pour assurer la sécurité et la confidentialité) à adopter pour faire face à la situation.

Sodexo doit suspendre le transfert de données s'il estime qu'aucune garantie appropriée pour un tel transfert ne peut être assurée, ou si le Responsable du Traitement ou l'Autorité de Contrôle compétente l'ordonne. Dans ce cas, l'entité Sodexo située en dehors de l'UE/EEE qui estime qu'elle est ou est devenue soumise à des réglementations ou pratiques non conformes aux exigences de la Politique en tant que Sous-traitant ne doit pas faire partie des BCR-ST.

Demande de communication des Données Personnelles par une autorité chargée de l'application de la loi ou un organisme de sécurité de l'état.

Si une entité de Sodexo reçoit ou prend connaissance d'une demande juridiquement contraignante de communication des Données Personnelles ou de tout accès direct aux Données Personnelles par une autorité chargée de l'application de la réglementation ou un organisme de sécurité de l'état, elle devra informer sans délai Sodexo SA, le Délégué à la Protection des Données du Groupe, et l'entité de Sodexo agissant en qualité d'Exportateur de Données.

L'entité de Sodexo agissant en tant qu'Exportateur de Données transmettra la notification au Responsable du Traitement et, si possible, à la Personne Concernée si le Responsable du Traitement le demande.

Sodexo évalue au cas par cas chaque demande d'accès aux données par toute autorité chargée de l'application de la loi ou organe de sécurité de l'état. Sodexo fait tout ce qui est en son pouvoir pour informer l'autorité requérante concernée des obligations de Sodexo au titre du RGPD et pour obtenir le droit de lever cette interdiction.

Sodexo met cette demande en attente pendant un délai raisonnable afin d'informer les parties prenantes de cette Politique en tant que Sous-traitant susmentionnées avant de divulguer les données à l'autorité requérante. Sodexo informe clairement les parties prenantes susmentionnées de la demande, y compris, mais sans s'y limiter, des informations sur les données demandées, le nombre de demandes, l'autorité requérante concernée et la base juridique de la divulgation.

Si dans des cas particuliers la suspension et/ou la notification sont interdites, Sodexo fait tout ce qui est en son pouvoir pour obtenir le droit de lever cette interdiction afin de communiquer le plus d'informations possibles et dans les meilleurs délais et pouvoir le démontrer, en documentant les meilleurs efforts mis en œuvre.

Si malgré tout Sodexo n'est pas en mesure d'informer les parties prenantes susmentionnées et de mettre la demande en attente, dans ce cas Sodexo fournit des informations générales sur les demandes qu'il a reçues aux parties prenantes susmentionnées (nombre de demandes de

communication, type de données demandées, autorité requérante si possible), dans la mesure où ladite autorité requérante l'a autorisée à communiquer ces informations à des tiers. L'entité Sodexo agissant en tant qu'Exportateur de Données transmettra ces informations au Responsable du Traitement.

En tout état de cause, le transfert de ces Données Personnelles à toute autorité publique ne peut être massif, disproportionné et aveugle d'une manière qui irait au-delà de ce qui est nécessaire dans une société démocratique.

Transferts transfrontaliers ou communications de données non-autorisés par la législation de l'Union

Pour les entités de Sodexo situées dans l'EEE, tout jugement d'une cour ou d'un tribunal et toute décision d'une autorité administrative d'un pays tiers exigeant qu'un Responsable du Traitement ou un Sous-traitant transfère ou divulgue des Données Personnelles ne peut être reconnu ou exécutoire de quelque manière que ce soit que s'il est fondé sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert conformément au Chapitre V du RGPD.

Toute entité Sodexo recevant une telle demande informera rapidement, conformément au contrat de service, au contrat ou à tout autre document contraignant conclu avec le Responsable du Traitement (un Client) :

- l'entité Sodexo agissant en tant qu'Exportateur de Données, qui transmettra la notification au Responsable du Traitement, qui a le droit de suspendre le transfert de Données Personnelles et/ou de résilier le contrat ou tout autre document contraignant avec Sodexo ; et,
- Sodexo SA ou,
- le délégué à la Protection des Données du Groupe et tout autre point de contact local dédié à la Protection des Données pertinent.

RÈGLE 24 - COOPÉRATION AVEC LES AUTORITÉS DE CONTRÔLE

RÈGLE 24 - Sodexo assiste le Responsable du Traitement dans l'exécution de son obligation de coopération avec les Autorités de Contrôle et conformément à la Procédure de Coopération des BCR

Dans le cadre de la Politique en tant que Sous-traitant, les entités de Sodexo assistent le Responsable du Traitement pour accomplir son obligation de coopérer avec les Autorités de Contrôle conformément à la procédure de coopération des BCR en Annexe 3 et, en particulier,

coopèrent et acceptent d'être auditées par les Autorités de Contrôle et de se conformer à l'avis de ces mêmes Autorités de Contrôle compétentes sur toute question liée à ces BCR.

RÈGLE 25 - ACTUALISATION DES BCR

RÈGLE 25 - Sodexo respecte la Procédure de mise à jour des BCR.

Conformément à la Procédure de mise à jour des BCR en Annexe 4, Sodexo signale une fois par an toute modification administrative de la Politique en tant que Sous-traitant ou de la liste des entités Sodexo membres des BCR aux Autorités de Contrôle concernées, via l'Autorité de Contrôle compétente (en l'occurrence la CNIL), avec une brève explication des motifs justifiant la mise à jour.

En cas de modifications importantes susceptibles d'affecter le niveau de protection offert par les BCR ou d'affecter de manière significative les BCR (c'est-à-dire des modifications du caractère contraignant), elles sont communiquées rapidement aux Autorités de Contrôle concernées, via l'Autorité de Contrôle compétente (la CNIL).

Toute modification des BCR est notifiée aux employés via l'intranet de Sodexo et aux autres Personnes Concernées et aux Responsables du Traitement sur le site internet officiel de Sodexo.

En cas de modification substantielle des BCR, Sodexo informe également le Responsable du Traitement de tout changement susceptible d'affecter les activités de traitement comme convenu contractuellement. Le Responsable du Traitement a la possibilité de s'opposer à une telle modification ou de résilier le contrat de service, le contrat ou tout autre document contraignant. Le Délégué à la Protection des Données du Groupe tient à jour une liste complète des entités Sodexo membres des BCR, avec le soutien de l'équipe juridique du Groupe. Il suit et enregistre toute mise à jour des BCR et fournit les informations nécessaires au Responsable du Traitement.

Sodexo s'assure qu'aucun transfert n'est effectué vers une nouvelle entité Sodexo tant que cette entité n'est pas effectivement liée par les BCR ou que toute autre garantie appropriée et n'est pas en mesure d'assurer la conformité.

RÈGLE 26 - CARACTERE CONTRAIGNANT DES BCR

RÈGLE 26 - Toutes les entités de Sodexo faisant partie du Groupe Sodexo agissant en tant que Sous-traitant se conforment à la Politique en tant que Sous-traitant, y compris leurs employés.

Lorsqu'elles agissent en tant que Sous-traitant, les entités de Sodexo qui ont adhéré à la Politique en tant que Sous-traitant, fournissent la Politique en tant que Sous-traitant au Responsable du Traitement dans le cadre du contrat de service, du contrat ou de tout autre document contraignant avec le Responsable du Traitement.

Lorsque les entités de Sodexo en tant que Sous-traitant sous-traitent leurs obligations, avec le consentement préalable du Responsable du Traitement, elles le font uniquement au moyen d'un accord écrit avec le sous-traitant ultérieur.

Lorsqu'un membre des BCR hors EEE cesse de faire partie du Groupe Sodexo ou d'être lié par les BCR, cette entité Sodexo continue d'appliquer les exigences des BCR au traitement des Données Personnelles qui lui ont été transférées au moyen des BCR, à moins que, au moment où il quitte le Groupe Sodexo ou cesse d'être lié par les BCR, ce membre supprime, anonymise ou restitue l'intégralité de ces Données Personnelles à une entité de Sodexo toujours liée par les BCR.

La Politique en tant que Sous-traitant a été partagée avec tous les employés en tant que nouvelle Politique de Protection des Données du Groupe et est disponible à tout moment sur l'intranet et le site internet officiel de Sodexo.

Tous les employés de Sodexo sont tenus d'assurer la confidentialité et de respecter les politiques de Protection des Données telles que définies dans la clause de Protection des Données incluse dans leur contrat de travail. Des sanctions disciplinaires ou des actions en justice appropriées peuvent s'appliquer en cas de non-respect de ces politiques de Protection des Données conformément à la loi.

04

Annexes



- Annexe 1 : Définitions
- Annexe 2 : Politique Globale de collecte et de conservation des données (Sous-traitant)
- Annexe 3 : Procédure de coopération des BCR
- Annexe 4 : Procédure de mise à jour des BCR
- Annexe 5 : Politique Globale relative à la protection des Données Personnelles de Sodexo
- Annexe 6 : Politique Globale de gestion des droits des Personnes Concernées
- Annexe 7 : Description du champ d'application matériel de la Politique en tant que Sous-traitant

Annexe 1 - Définitions

Lorsque l'objet des présentes définitions concerne des Données Personnelles, les termes et expressions sans majuscule utilisés, par exemple, « Données Personnelles », « traitement », etc., seront interprétés conformément au sens qui leur est donné dans le RGPD. En outre, les termes en majuscules énoncés dans les présentes définitions auront, aux fins des présentes BCR, la signification qui leur est attribuée ci-dessous.

- **Autorité de Contrôle** désigne une autorité publique indépendante établie par un Etat Membre, comme spécifié dans le RGPD.
- **CEPD** désigne le Comité Européen de la Protection des Données. Il s'agit d'un organisme européen indépendant, qui contribue à l'application cohérente des règles de Protection des Données dans toute l'Union européenne et promeut la coopération entre les autorités de Protection des Données de l'UE.
- **Client** désigne les organisations ou sociétés externes établies dans l'UE ou l'EEE, qui demandent au Groupe Sodexo d'exécuter des services en leur nom pour leurs employés / leur personnel sur site, qui sont les utilisateurs finaux de ces services, il s'agit du Responsable du Traitement.
- **Délégué à la Protection des Données du Groupe** désigné la personne nommée avec l'aval du comité de direction du Groupe Sodexo pour superviser les questions de confidentialité des données au niveau du Groupe Sodexo et pour définir et diffuser le programme de conformité de Sodexo en matière de Protection des Données et les bonnes pratiques relatives à la confidentialité des données et assurer leur mise en œuvre conformément à la Règle 20.
- **Données Personnelles** Les Données Personnelles désignent toute information relative à une personne physique identifiée ou identifiable ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.
- **Données Personnelles Sensibles** désignées comme « Catégories Particulières de Données Personnelles » au sens du RGPD désigne toute donnée personnelle révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et le traitement des données génétiques, des données biométriques aux fins d'identifier de manière unique une personne physique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Cette définition inclut également les Données Personnelles relatives aux infractions et aux condamnations pénales.
- **EEE** signifie l'Espace Economique Européen.

- **Exportateur de Données** désigne un Responsable du Traitement (ou si autorisé, un Sous-traitant) établi dans l'UE qui transfère des Données Personnelles à un Importateur de Données.
- **Groupe Sodexo ou entité de Sodexo ou entités de Sodexo ou membres de la Politique en tant que Sous-traitant** désigne toute société ou participation économique détenue directement ou indirectement par Sodexo à hauteur au moins de 50 % du capital social et des droits de vote et qui est soumise aux Règles d'Entreprise Contraignantes de Sodexo.
- **Importateur de Données** désigne un Responsable du Traitement ou un sous-traitant situé dans un pays tiers qui reçoit des Données Personnelles de l'Exportateur de Données.
- **Pays adéquat** ; désigne un pays qui assure un niveau de protection adéquat selon une « décision d'adéquation » adoptée par la Commission européenne, cette dernière ayant le pouvoir de déterminer si un pays tiers assure un niveau de protection adéquat des Données Personnelles en raison de sa législation nationale ou les engagements internationaux qu'il a contractés
- **Personne Concernée** désigne une personne physique identifiée ou identifiable dont les Données Personnelles sont concernées par un traitement au sein du Groupe Sodexo, y compris les Données Personnelles des candidats, employés, clients, consommateurs/bénéficiaires, fournisseurs/vendeurs, prestataires/sous-traitants, ou tout autre tiers.
- **Point de contact local dédié à la Protection des Données** désigne la personne désignée par une entité Sodexo, chargée de traiter les questions relatives à la Protection des Données et de la confidentialité des données à l'échelle locale. Dans certains cas, le point de contact local dédié à la Protection des Données peut être nommé Délégué local à la Protection des Données lorsque la législation applicable en matière de Protection des Données l'exige.
- **Programme Global de Protection des Données de Sodexo** désigne le programme présenté et validé par le Délégué à la Protection des Données du Groupe au comité de direction du Groupe Sodexo.
- **Règlement général sur la Protection des Données ou RGPD** désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du Traitement des Données Personnelles et à la libre circulation de ces données, abrogeant la Directive 95/46/CE.
- **Responsable du Traitement** désigne l'entité qui détermine les finalités et les moyens du traitement des Données Personnelles.
- **Sous-traitant** désigne la personne physique ou morale, l'agence ou tout autre organisme qui traite des Données Personnelles pour le compte du Responsable du Traitement.

- **Traitement ou Traitement des Données Personnelles** désigne toute opération ou ensemble d'opérations effectuées sur des Données Personnelles ou sur des ensembles de Données Personnelles, par des moyens automatisés ou non, tels 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 tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- **UE** signifie l'Union Européenne.

- **Violation des Données Personnelles** désigne toute violation de la sécurité entraînant la destruction accidentelle ou illégale, la perte, l'altération, la divulgation ou l'accès non autorisé aux Données Personnelles transmises, stockées ou autrement traitées.

Annexe 2 - Politique Globale de collecte et de conservation des données (Sous-traitant)

PRÉAMBULE

Sodexo s'engage à protéger la vie privée de ses employés, clients, consommateurs et de toute autre personne et a mis en place des politiques, programmes et pratiques de confidentialité solides. En particulier, lorsque Sodexo, en tant que Sous-traitant, effectue un Traitement de Données Personnelles selon les instructions documentées d'un Responsable du Traitement.

Afin de respecter les meilleures pratiques en matière de conservation des Données Personnelles, Sodexo a adopté une Politique Globale de Conservation des Données. La présente Politique décrit comment Sodexo, lorsqu'il agit en tant que Sous-traitant, suit les principes du RGPD et de toute autre loi applicable et donc comment Sodexo assure la protection des droits et libertés des individus.

DÉFINITIONS

- **Données Personnelles** désignent toute information relative à une personne physique identifiée ou identifiable ; une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments propres à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.
- **Entité de Sodexo ou entités de Sodexo** désigne toute société, société de personnes ou autre entité ou organisation admise de temps à autre en tant que membre du Groupe Sodexo.
- **Personne concernée** désigne une personne physique identifiée ou identifiable dont les Données Personnelles sont concernées par un traitement au sein du Groupe Sodexo, y compris les Données Personnelles des candidats, employés, clients, consommateurs/bénéficiaires, fournisseurs/vendeurs, prestataires/sous-traitants, ou tout autre tiers.
- **Règlement général sur la Protection des Données ou RGPD** désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46 /CE.
- **Responsable du Traitement** désigne la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des Données Personnelles. Dans cette politique, le Responsable du Traitement signifie un Client.

- **Traitement des données personnelles** désigne toute opération ou ensemble d'opérations effectuées sur des données personnelles ou sur des ensembles de données personnelles, par des moyens automatisés ou non, tels 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, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

COMMENT AIDER LE RESPONSABLE DU TRAITEMENT À SE CONFORMER AUX EXIGENCES DE LIMITATION DE CONSERVATION

- a. Se conformer à l'instruction du responsable du traitement concernant la durée de conservation des données personnelles

Le sous-traitant doit toujours se conformer aux instructions du responsable du traitement lors du traitement des données personnelles. Ceci s'applique également à la suppression des données personnelles à la fin du cycle de vie du traitement.

Les données personnelles seront donc toujours conservées et/ou supprimées et/ou anonymisées selon les instructions du responsable du traitement conformément à la période de conservation des données personnelles qu'il a fixées, sous réserve que ces instructions soient conformes aux lois locales applicables.

Sodexo et ses sous-traitants ultérieurs (le cas échéant) demanderont au responsable du traitement d'opter pour la suppression, le retour ou l'anonymisation des données personnelles. Le choix sera spécifié dans le contrat ou tout autre document contraignant avec ce responsable du traitement.

Sodexo dispose des données personnelles de manière sécurisée conformément à la Politique de Sécurité des Systèmes d'informations du Groupe

- b. Résiliation du contrat

Sodexo et ses sous-traitants ultérieurs (le cas échéant) demanderont au responsable du traitement de faire un choix entre la suppression, le retour ou l'anonymisation des données personnelles. Le choix sera spécifié dans le contrat ou tout autre document contraignant avec ce responsable du traitement.

À la fin de la fourniture des services relatifs au traitement des données personnelles, Sodexo, en tant que sous-traitant et ses sous-traitants (le cas échéant), agiront conformément au choix du responsable du traitement exprimé dans le contrat et supprimeront, anonymiseront ou restitueront toutes les données personnelles transférées et leurs copies au responsable du traitement et démontreront qu'elles l'ont fait en fournissant une attestation au responsable du traitement. Cette attestation doit comporter au moins la date de suppression ou d'anonymisation de la liste des données personnelles supprimées ou anonymisées et la signature du chef d'entreprise concerné

et du délégué à la protection des données ou du point de contact local dédié à la Protection des Données. Si les lois locales applicables définissent une période de conservation obligatoire des données personnelles et exigent que Sodexo conserve les données personnelles en conséquence, Sodexo devra garantir la confidentialité des données personnelles et ne traitera plus activement les données personnelles, sauf dans la finalité pour laquelle elles sont légalement conservées.

Si le responsable du traitement n'a pas exprimé contractuellement son choix, Sodexo demandera au responsable du traitement de communiquer sa décision concernant les données personnelles au plus tard à la date de résiliation du contrat.

Enfin, Sodexo agissant en tant que sous-traitant informera chaque entité Sodexo à laquelle le traitement des données personnelles a été sous-traité de toute suppression ou anonymisation des données et demandera à chaque entité Sodexo susmentionnée d'en faire de même.

Annexe 3 - Procédure de coopération des BCR

1. La présente procédure de coopération définit la manière dont les entités de Sodexo adhérant aux BCR doivent coopérer avec leurs autorités de contrôle compétentes pour toute demande ou question liée à la mise en œuvre, l'interprétation ou l'application des BCR.
2. Les entités de Sodexo adhérant aux BCR mettent à disposition le personnel nécessaire pour dialoguer avec les autorités de contrôle compétentes.
3. Les entités de Sodexo adhérant aux BCR doivent se conformer à toute décision ou avis émis par les autorités de contrôle compétentes sur toute question relative à la législation sur la protection des données susceptible d'affecter la mise en œuvre, l'interprétation ou l'application des BCR.
4. Les entités de Sodexo adhérant aux BCR doivent activement examiner et prendre en compte les directives, recommandations et meilleures pratiques émises ou approuvées par le Comité Européen de la Protection des Données qui peuvent affecter la mise en œuvre, l'interprétation ou l'application des BCR.
5. Les entités de Sodexo adhérant aux BCR s'engagent à se soumettre à une décision formelle des autorités de contrôle compétentes, sur toute question liée à la mise en œuvre, l'interprétation ou l'application des BCR.
6. Les entités de Sodexo adhérant aux BCR doivent communiquer sans délai aux autorités de contrôle compétentes toute modification significative des BCR conformément à la Procédure de mise à jour des BCR (Annexe 4 des BCR).
7. Les entités de Sodexo adhérant aux BCR doivent répondre à toute demande d'information ou réclamation émanant des autorités de contrôle compétentes.
8. Sur demande, les entités de Sodexo adhérant aux BCR doivent fournir aux autorités de contrôle compétentes une copie des résultats de toute évaluation de la conformité aux BCR et/ou de toute autre documentation requise, et la capacité de mener un audit des entités Sodexo adhérant aux BCR dans le but d'examiner la conformité aux BCR.

Annexe 4 - Procédure de mise à jour des BCR

PRÉAMBULE

1. La présente procédure de mise à jour définit la manière dont Sodexo communiquera les modifications apportées aux BCR aux autorités de contrôle compétentes, aux clients, aux personnes concernées et aux entités de Sodexo adhérant aux BCR.

Changements substantiels

2. Sodexo communiquera rapidement toute modification substantielle des BCR (entendue comme toute modification susceptible d'affecter le niveau de protection offert par les BCR ou susceptible d'affecter de manière significative les BCR, telle qu'une modification du caractère contraignant des BCR) aux autorités de contrôle concernées via la Commission Nationale de l'Informatique et des Libertés (« CNIL »), agissant en qualité d'autorité de contrôle chef de file de Sodexo.
3. Lorsqu'une modification substantielle des BCR affecte les conditions dans lesquelles Sodexo traite les données personnelles pour le compte d'un client en vertu d'un contrat ou d'un autre document contraignant que Sodexo a signé avec ce client, Sodexo doit :
 - a. Communiquer le changement proposé avant de le mettre en œuvre, et avec un préavis suffisant pour permettre au Client concerné de s'y opposer ; et
 - b. Permettre au Client de suspendre le transfert de données personnelles à Sodexo et/ou de mettre fin à sa relation avec Sodexo, conformément aux termes de son contrat ou de tout autre document contraignant avec Sodexo

Changements administratifs

4. Sodexo communiquera les modifications des BCR qui sont de nature administrative (y compris les modifications de la liste des entités de Sodexo adhérant aux BCR) aux autorités de contrôle concernées, via la CNIL au moins une fois par an. Sodexo fournira également une brève explication des motifs de tout changement administratif communiqué apporté aux BCR.

Communication aux personnes concernées et aux entités de Sodexo adhérant aux BCR

5. Sodexo communiquera dans les meilleurs délais toutes les modifications des BCR, qu'elles soient de nature administrative ou substantielle, aux entités de Sodexo adhérant aux BCR et aux Clients.
6. Sodexo communiquera les changements administratifs ou substantiels aux personnes concernées qui bénéficient des BCR via l'intranet et le site internet officiel de Sodexo.

Rôle du Délégué à la protection des données du Groupe

7. Le Délégué à la protection des données du Groupe, avec le soutien de l'équipe du Délégué à la protection des données de Groupe, (i) tiendra à jour une liste complète des entités de Sodexo adhérant aux BCR et des sous-traitants impliqués dans les activités de traitement des données pour le compte des Clients (agissant en tant que responsable du traitement) ; (ii) mettra à disposition des Clients (agissant en tant que responsable du traitement), des personnes concernées et des autorités de contrôle la liste entièrement mise à jour susmentionnée ; et (iii) suivra et enregistrera toute mise à jour des BCR et fournira systématiquement les informations nécessaires aux Clients (agissant en tant que responsable du traitement) et/ou aux autorités de contrôle sur demande.
8. Sodexo s'assure qu'aucun transfert n'est effectué vers une nouvelle entité de Sodexo tant que cette entité n'est pas efficacement liée par les BCR ou toute autre garantie appropriée et ne peut pas assurer la conformité avec les BCR.

Annexe 5 - Politique Globale relative à la protection des Données Personnelles de Sodexo

Lien vers la Politique globale relative à la protection des données de Sodexo publiée sur le site internet officiel de Sodexo SA.

Annexe 6 - Politique Globale de gestion des droits des Personnes Concernées

Lien vers la Politique Globale de gestion des droits des Personnes Concernées publiée sur le site internet officiel de Sodexo SA

Annexe 7 - Description du champ d'application matériel de la Politique en tant que Sous-traitant

Types de Traitement de Données Personnelles effectués et/ou envisagés et finalités	Catégories des Personnes Concernées	Catégories des Données Personnelles ayant fait l'objet d'un Traitement	Liste des pays de destination
<ul style="list-style-type: none"> ■ Exécution des services fournis par Sodexo pour le compte des Clients (ex : services de gestion des installations, services de restauration, certains des services avantages et récompenses¹¹). 	<ul style="list-style-type: none"> ■ Clients (contacts commerciaux actuels ou potentiels) ■ Consommateurs/Bénéficiaires (consommateurs ou bénéficiaires actuels ou potentiels) 	<ul style="list-style-type: none"> ■ Données d'identification (état civil, identité...) ■ Vie professionnelle ■ Données de connexion (ex : informations d'identification à des fins d'authentification, logs/interaction avec les applications informatiques pertinentes, adresse IP) 	<ul style="list-style-type: none"> ■ Tous les pays où les entités de Sodexo opèrent.

¹¹ Services fournis par Sodexo pour le compte de Clients :

- Services sur Site :
 - Services alimentaires : restauration, cafétéria, restaurants spéciaux, commerces de détail et distributeurs automatiques ;
 - Services de gestion des installations :
 - Services de Soft FM nettoyage, blanchisserie, réception, service d'assistance, sécurité ;
 - Hard FM : maintenance technique, maintenance électrique, maintenance des bâtiments.
- Services Avantages et Récompenses :
 - Avantages aux employés : Sodexo développe le Pass Repas ou le Pass Cadeau pour attirer et fidéliser les collaborateurs et améliorer l'efficacité de l'organisation
 - Diversification : Sodexo propose des solutions simples et faciles d'accès pour répondre aux enjeux de mobilité, de santé et de bien-être, d'incitation et de reconnaissance via des plateformes uniques telles que les cartes carburant, la réservation de voyages Mobility Pass et la gestion des frais professionnels.

Selon la réglementation locale, pour ces services, les entités Sodexo peuvent être considérées comme des sous-traitants.

